Online Safety and Acceptable Use of Technology Policy for Educational Settings

September 2020

Kent County Council
kent.gov.uk

THE EDUCATION PEOPLE

Contents

Acceptable Use of Technology Policy (AUPs) Template Content

Using the Policy Template: Guidance Notes

This template aims to provide educational settings with a framework to develop their online safety ethos and enable leaders and managers to detail strategic approaches and considerations with regards to the safer use of technology within their settings.

The online safety policy should be recognised by educational settings as part of the portfolio of safeguarding policies; it is not a technical or computing policy and as such should fall within the role and responsibilities of the lead Designated Safeguarding Lead (DSL). The DSL is however likely to require advice and support from other staff within the setting to ensure the policy is robust and accurate; leaders should ensure that enough time is allocated to DSLs to ensure this takes place.

We encourage all educational settings to use the following statements but ensure that their online safety policy is individualised for their specific context. It will not be appropriate for educational settings to adopt this template in its entirety as some statements will be more relevant to some settings than others; DSLs and leaders should ensure unnecessary content is removed.

Leaders, managers and DSLs should adapt the content to include specific local information such as their own named points of contact, as well as specific procedures and expectations. These decisions and details will vary from setting to setting, so this template should be used as a starting framework.

- **Blue font** indicates that the setting should insert relevant information
- **Pink font** highlights suggestions to assist DSLs, leaders and managers in amending sample statements and ensuring content is appropriate for their setting. This content is provided as guidance notes and should not be left in individual settings policies.

There is no requirement for educational settings to have a separate online safety policy, however online safety aspects such as use of social media and mobile technology need to be appropriately addressed by settings. This could be within a specific online safety policy, standalone policies or embedded within existing documents. The decision regarding how to manage this is down to leaders and managers; if online safety is embedded within existing documents, settings should ensure that the whole community is aware of how and where to locate information, especially regarding online behaviour expectations and responding to and reporting specific online safety concerns.

Disclaimer

The Education People make every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by The Education People. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the Education People copyright is acknowledged and we are informed of its use.

East Stour Primary School
Online Safety Policy

Key Details

Designated Safeguarding Lead (s): Emma Law

Named Governor with lead responsibility: Sam Newton

Date written: November 2020

Date agreed and ratified by Governing Body:

Date of next review: November 2021

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

East Stour Online Safety Policy

1. Policy aims

- This online safety policy has been written by East Stour, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

- The purpose of East Stour online safety policy is to
  - safeguard and promote the welfare of all members of East Stour community online.
  - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.

- East Stour identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk.
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy scope

- East Stour recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- East Stour identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- East Stour will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
  - o Behaviour and Anti-bullying policy
  - o Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
  - o Child protection policy
  - o Confidentiality/GDPR policy
  - o Curriculum policies/progression maps, such as Relationships and Sex Education (RSE)
  - o Cameras and image use policy
  - o Mobile phone and social media policies
  - o Searching, screening and confiscation policy

3. Monitoring and review

- Technology evolves and changes rapidly; as such East Stour will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (*Emma Law - Headteacher*) is recognised as holding overall lead responsibility for online safety.
- East Stour recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.

- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the school management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

- Meet regularly (Bi-annually as a minimum) with the governor with a lead responsibility for safeguarding and/or online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including passwords and encryption as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.

- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
  - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
  - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study. (Resources used from Think You Know website and CEOP)
  - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
  - implementing appropriate peer education approaches.
  - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
  - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.

  - making informed decisions to ensure that any educational resources used are appropriate for our learners.
  - using external visitors, where appropriate, to complement and support our internal online safety education approaches. *Using External Visitors to Support Online Safety Education: Guidance for Educational Settings*
  - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
  - rewarding positive use of technology.

- East Stour will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
  - displaying acceptable use posters in all rooms with internet access.
  - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- East Stour will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
  - ensuring age appropriate education regarding safe and responsible use precedes internet access.
  - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- East Stour recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- East Stour will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.

- Staff at East Stour will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teachers to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 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 which is integrated, aligned and considered as part of our overarching safeguarding approach. This will form part of our annual safeguarding training for all staff.
  - Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
  - build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
  - highlight useful educational resources and tools which staff could use with learners.
  - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- East Stour recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by
  - providing information and guidance on online safety in a variety of formats, such as online safety events, parent evenings, transition events, fetes and sports days.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- East Stour recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will
  - regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- East Stour uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices
  - Internet, which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- (Staff will ensure that if they access Google Mail on classroom devices they will log off to avoid children staff accounts)
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use appropriate search tools as identified following an informed risk assessment. (Google safe search)
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners age and ability.
  - **Early Years Foundation Stage and Key Stage 1**

    - 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 learners age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

7.3 Filtering and monitoring

www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

7.3.1 Decision making

- East Stour governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- East Stour's education broadband connectivity is provided through EIS and the KPSN
- East Stour uses Light Speed
  - Light Speed blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

  - Light Speed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
  - Light Speed integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with Light Speed to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to
  - turn off monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches we will:
  - Upload to My Concern

7.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
  - Full information can be found in our GDPR policy which can be accessed at via the website.

7.5 Security and management of information systems

We take appropriate steps to ensure the security of our information systems, including:

  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.

  - o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - o Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
  - o Checking files held on our network, as required and when deemed necessary by leadership staff.
  - o The appropriate use of user logins and passwords to access our network.
    - ▪ Specific user logins and passwords will be enforced for all users from KS2 upwards.
  - o All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 3 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
  - o use strong passwords for access into our system.
  - o change their passwords every academic year
  - o not share passwords or login information with others or leave passwords/login details where others can find them.
  - o not to login as another user at any time.
  - o lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the Headteacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents. A 7.30pm to 7,30am and no weekend email request is in place across the school. Members of staff are welcome to make individual arrangements with colleagues.

7.8.2 Learner email

- Learners will use a provided email account for educational purposes.
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses will be used for communication outside of the setting.

7.9 Educational use of videoconferencing and/or webcams

- East Stour recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing 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 details will not be posted publicly.
  - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
  - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
  - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of learning platforms

- East Stour does not currently use an online learning platform. If they did:
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.

- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.

- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

7.11 Management of applications (apps) used to record children's progress

- We use EExAT to track learners progress and share appropriate information with parents and carers in EYFS.
- The EYFS Lead will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
    - only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of East Stour community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of East Stour community are expected to engage in social media in a positive and responsible manner.
    - All members of East Stour community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

- We will control learner and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during *school* hours for personal use is only permitted for staff during their break times.
    - The use of social media during school hours for personal use is not permitted for learners.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.
- Concerns regarding the online conduct of any member of East Stour community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our code of conduct/safeguarding induction.

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of East Stour on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.

- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

8.2.2 Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Headteacher.
  - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy)

8.3 Learners use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
  - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
  - to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
  - to use safe passwords.
  - to use social media sites which are appropriate for their age and abilities.
  - how to block and report unwanted communications.

  - how to report concerns on social media, both within the setting and externally.

8.4 Official use of social media

- East Stour official social media channels are:
  - Twitter
- The official use of social media sites by East Stour only takes place with clear educational or community engagement objectives and with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage official social media channels.
  - Official social media sites are suitably protected and, where possible, run and/or linked to our website.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

8.4.1 Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our social media acceptable use policy.

- Be aware they are an ambassador for the setting.
- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- East Stour recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of East Stour community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of East Stour community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as toilets and classrooms.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of East Stour community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, data security and acceptable use of technology.
    - keep mobile phones and personal devices in a safe and secure place (locker/locked cupboard) during lesson time.
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - not use personal devices during teaching periods, unless written or verbal permission has been given by the headteacher such as in emergency circumstances.
    - ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy)
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and will only use work-provided equipment for this purpose.
    - directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.3 Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - East Stour expects learners' personal devices and mobile phones to be locked in the school office
- If a learner needs to contact his/her parents or carers the setting will do so on their behalf.
    - Parents are advised to contact their child via the school office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

  - o If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
  - o Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
  - o Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
  - o Searches of mobile phone or personal devices will be carried out in accordance with the DfE 'Searching, Screening and Confiscation' guidance.
  - o Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. This is in line with the DfE 'Searching, Screening and Confiscation' guidance.
  - o Mobile phones and devices that have been confiscated will be released to parents/ carers.
  - o If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, should ensure that Mobile phones are kept in bags or locked away on arrival.
- Appropriate signage and information is provided to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) of any breaches of our policy.

10. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

  - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- East Stour recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Headteacher in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL (or deputy).The headteacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.

- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

- Our headteacher, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- East Stour 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
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- 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 any concerns relating to 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 learners personal 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 implementing safety plans, offering advice on blocking, reporting and removing online content, and 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 referrals to partner agencies, such as Children's Social Work Service and/or the police.
  - if the concern involves children and young people at a different educational setting, the DSL will 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 the 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.
- East Stour 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.
- East Stour recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, East Stour 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- East Stour recognises youth produced sexual imagery (also known as "sexting") as 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 UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".
  - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
  - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- East Stour will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- 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 suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.

        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video 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 local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially 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 in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP 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 UKCIS 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.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- East Stour recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- East Stour will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.

- We will implement preventative approaches for online child abuse and 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 abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community. This can be found on our website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP procedures.
    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner 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 and provide support and signposting, as appropriate.
    - 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 abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: 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 Service and/or 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 police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- East Stour will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- 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 (IWF) 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 the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
  - act in accordance with our child protection policy and the relevant KSCMP procedures.
  - store any devices involved securely.
  - immediately inform appropriate organisations, such as the IWF and police.
- 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 IWF 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 IWF via www.iwf.org.uk .
  - inform the police via 101 or 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) following a written request from the police.
  - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
  - ensure that the headteacher is informed in line with our managing allegations against staff policy.
  - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
  - quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at East Stour.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy found on our website.

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at East Stour and will be responded to in line with existing policies, including child protection, 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 Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

December 2020

Responding to an Online Safety Concern Flowchart

Key Local Contacts

Designated Safeguarding Lead (s):
Name, Role and contact info

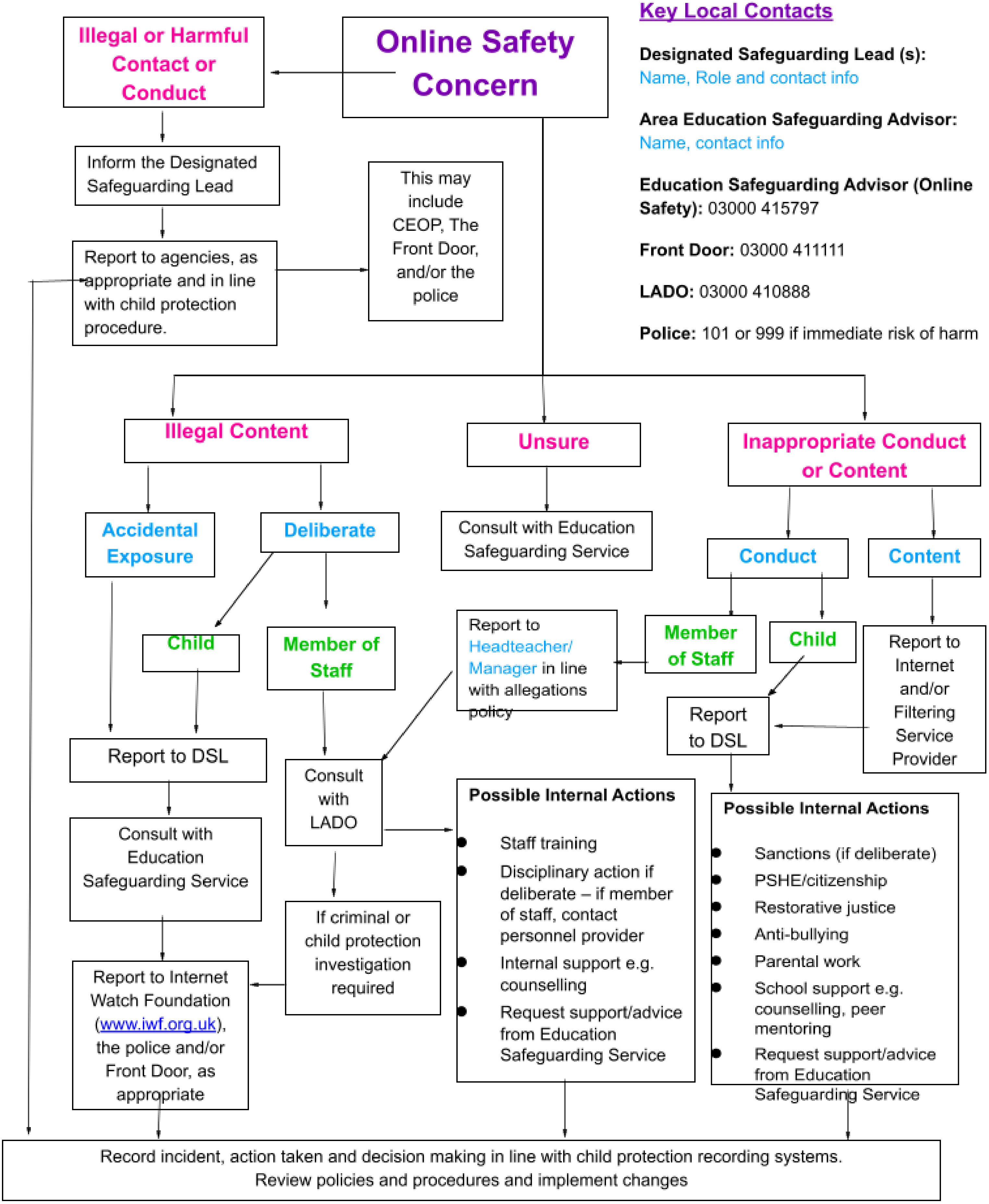
Area Education Safeguarding Advisor:
Name, contact info

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, The Front Door, and/or the police

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Consult with LADO

If criminal or child protection investigation required

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or Front Door, as appropriate

Unsure

Consult with Education Safeguarding Service

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to Headteacher/ Manager in line with allegations policy

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

Record incident, action taken and decision making in line with child protection recording systems.
Review policies and procedures and implement changes

Useful Links

Kent Educational Setting Support and Guidance

Education Safeguarding Service, The Education People:

- 03000 415797
  - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
  - Ashley Assiter, Online Safety Development Officer
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For non-urgent enquiries, contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services:
www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eisit.uk

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

Acceptable Use of Technology Policy (AUP) Templates

Using the AUP Templates: Guidance Notes

The following content is provided as suggestions and guidance only to support educational settings in creating Acceptable Use of Technology Policies (AUPS) which are relevant to their communities. It is recommended that settings ensure their AUP reflects the needs and abilities of their learners, their community and the technology available.

Settings will need to adapt these templates in line with their own technology use, for example the expectations or requirements may vary if settings use laptops or tablets. Where possible and appropriate, learners, staff and parents/carers should be directly involved in this process.

- **Blue font** indicates that the setting should insert relevant information
- **Pink font** highlights suggestions to assist DSLs, leaders and managers in amending sample statements and ensuring content is appropriate for their setting. This content is provided as guidance notes and should not be left in individual settings policies

Learner Acceptable Use of Technology Sample Statements

Although statements for learners are collected within key stages, it is recommended that settings amend and adapt them according to their own cohorts needs. The template statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with learners and amend them to develop ownership and understanding.

Early Years and Key Stage 1 (0-6)

I understand that the school Acceptable Use Policy will help keep me safe and happy online.

- Where pupils are using their own devices for remote learning we would expect adult supervision as necessary. In school devices will have appropriate age restrictions and be under adult supervision
- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets and use of programmes including purple mash and seesaw, including when I am at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules:
  - I may have limited access to devices

  - I may need an adult to work with me when I am online
  - My parents/carers will be spoken to

I have read and talked about these rules with my parents/carers

Shortened version (for use on posters)

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

Key Stage 2 (7-11)

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission
- I only talk with and open messages from people I know
- I will only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Learning

- As a school we use Seesaw for online work and children and parents have access to the app. This is monitored by school staff. Google drive is available for staff and we plan to roll this out to KS2.
- I ask my teacher before using my own personal devices at school. This will only be available on specific request by the teacher and linked to school learning.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I keep my personal information safe and private online.

- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I know that if I do not follow the school rules then:
    - I will be closely monitored by adult for further use
    - I may not have access to the internet for set periods of time
    - An adult from home will be informed

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page or close the screen and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to any adult in my class.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Alternative KS2 Statements *(With thanks to Kingsnorth Primary School)*

- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.

- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in memory sticks / CDs from outside of school, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.*.*
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I know that all school devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened KS2 version (for use on posters)

- I ask a teacher about which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up, I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

Learners with SEND

Learners with SEND functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I don't like online, I tell a grown up
- I know that if I do not follow the school rules then:

    - I will be closely monitored by adult for further use
    - I may not have access to the internet for set periods of time
    - An adult from home will be informed

Learners with SEND functioning at Levels P7-L1

(Based on Childnet’s SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- On the internet I don’t tell strangers my name
- I know that if I do not follow the school rules then:
    - I will be closely monitored by adult for further use
    - I may not have access to the internet for set periods of time
    - An adult from home will be informed

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I don’t open emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see anything that I don’t like online, I will tell a grown up

Learners with SEND functioning at Levels L2-4

(Based on Childnet’s SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then:
- I will be closely monitored by adult for further use
- I may not have access to the internet for set periods of time
- An adult from home will be informed

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

Accepting

- I don't open messages from strangers
- I check web links to make sure they are safe

Reliable

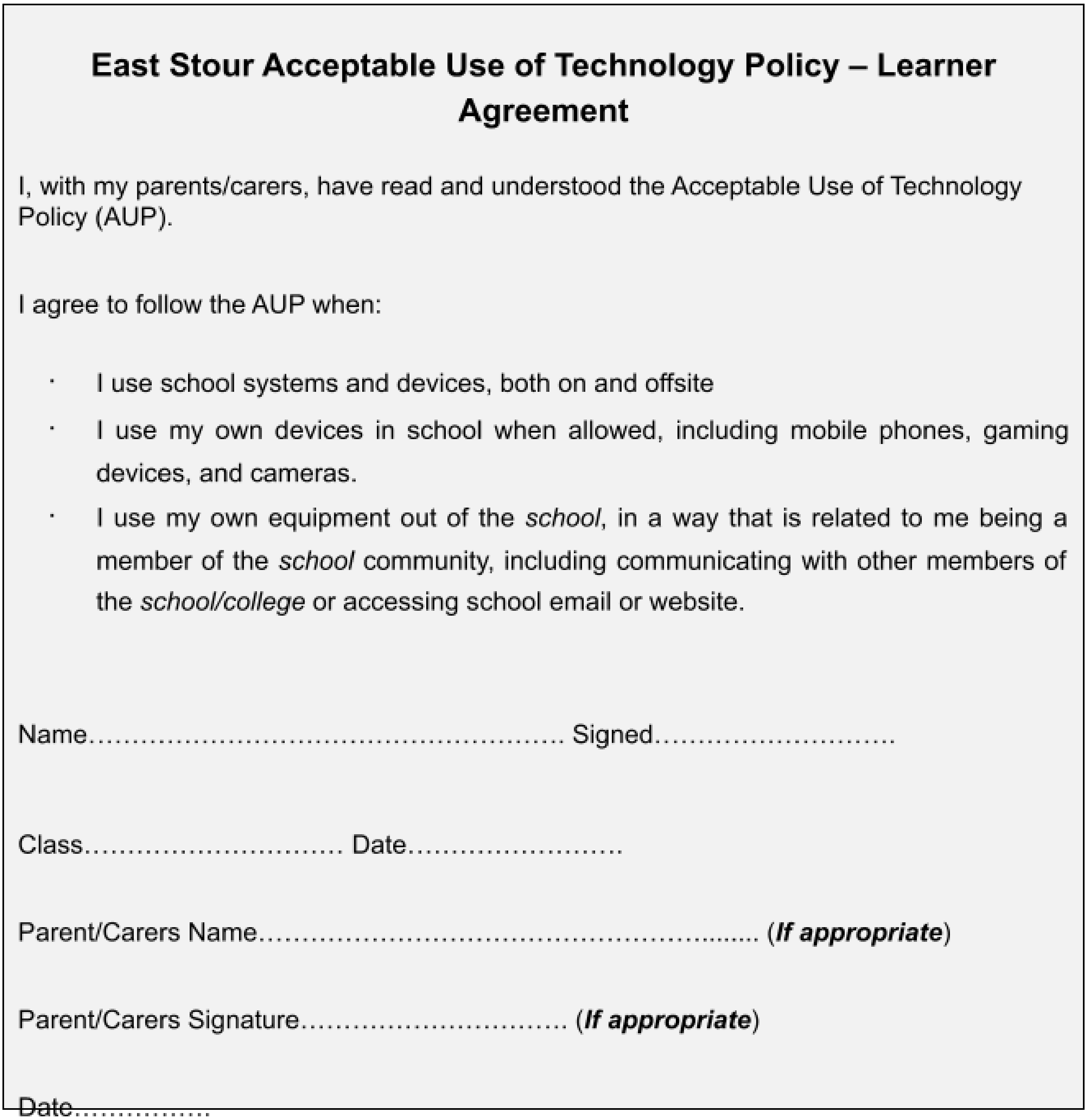
- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see anything online that I don't like, I will tell a teacher

Learner Acceptable Use Policy Agreement Form

Settings should attach a copy of the AUP to this form.



East Stour Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

- I use school systems and devices, both on and offsite
- I use my own devices in school when allowed, including mobile phones, gaming devices, and cameras.
- I use my own equipment out of the *school*, in a way that is related to me being a member of the *school* community, including communicating with other members of the *school/college* or accessing school email or website.

Name……………………………………………… Signed………………………

Class………………………… Date……………………

Parent/Carers Name…………………………………………….......... (***If appropriate***)

Parent/Carers Signature………………………… (***If appropriate***)

Date…………….

Acceptable Use of Technology Sample Statements/Forms for Parents/Carers

Parent/Carer Acknowledgement Form

East Stour Primary School Learner Acceptable Use of Technology Policy Acknowledgment

Settings should attach a copy of an age appropriate AUP to this form. Settings may need to provide parents with updated versions of the AUP as learners progress through the setting.

1. I, with my child, have read and discussed the East Stour learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

3. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

4. I am aware that the school mobile technology policy states that my child cannot use personal device and mobile technology on site. Unless requested by staff as part of their leanring.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

8. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

10. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name………………………………… Child's Signature ………………………………... (*if appropriate*)

Class………………………… Date……………………

Parents Name……………………………………………….....................................

Parents Signature……………………………………………………………….. Date……………

Sample Parent/Carer Acceptable Use of Technology Policy

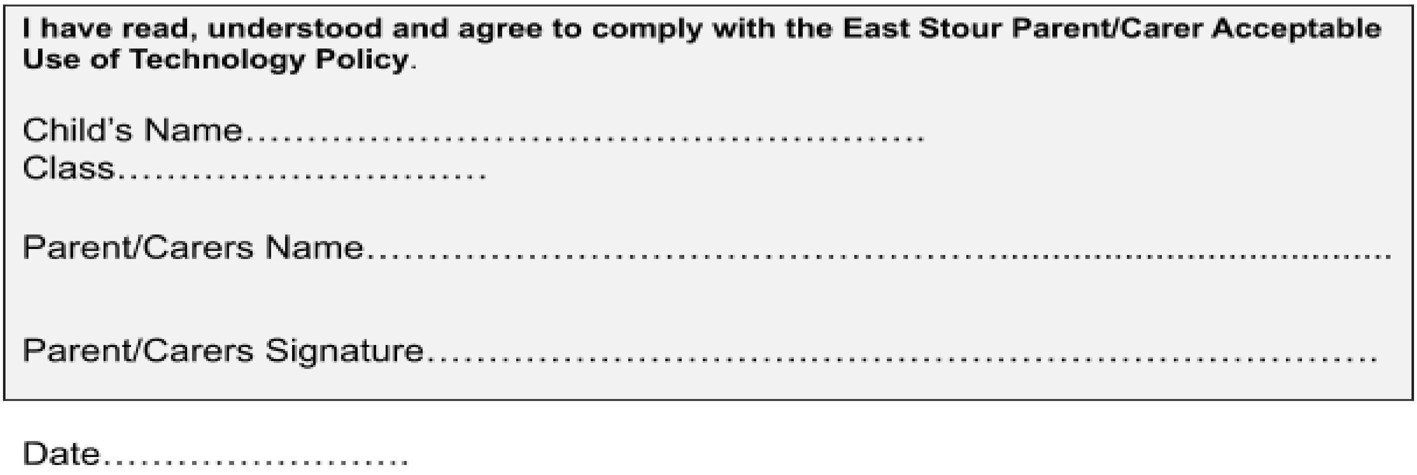
Issues for learning could be created if parents/carers refuse to sign an AUP as children need to use the internet to access the curriculum. Setting should have a robust process in place to manage and record parental responses and to engage with parents/carers who do not respond. Alternatives include highlighting online safety within the Home School Agreement or using an acknowledgement form.

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at East Stour.
2. I am aware that learners use of mobile technology and devices, such as mobile phones, is not permitted at East Stour unless requested for a directed activity.
3. I am aware that any internet and technology use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the school systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the school internet and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed.

6. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
7. I have read and discussed East Stour learner Acceptable Use of Technology Policy (AUP) with my child.
8. I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.
9. I know I can seek support from the school about online safety, such as via the school website to help keep my child safe online at home.
10. I will support the school/ approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text and video online responsibly.
11. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
12. I understand that a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.

13. I understand that if I or my child do not abide by the East Stour AUP, appropriate action will be taken. This could include sanctions being applied in line with the school policies:
    - I will be closely monitored by adult for further use
    - I may not have access to the internet for set periods of time
    - An adult from home will be informed
    - and if a criminal offence has been committed, the police being contacted.
14. I know that I can speak to the Designated Safeguarding Lead Emma Law – Headteacher, my child's teacher or a member of the SLT if I have any concerns about online safety.



I have read, understood and agree to comply with the East Stour Parent/Carer Acceptable Use of Technology Policy.

Child's Name...
Class..............................

Parent/Carers Name..

Parent/Carers Signature...

Date........................

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use East Stour IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand East Stour expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within East Stour both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and online and offline communication technologies**.**

2. I understand that East Stour Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed within reason.

6. Where I deliver or support remote learning, I will comply with the school remote learning AUP and protocols.

Data and System Security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
   - I will use a 'strong' password to access *school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Leaders should include any specific requirements, for example, how often passwords should be changed etc.*
   - *I will protect the devices in my care from unapproved access or theft. For example not leaving devices visible or unsupervised in public places.*

8. I will respect school system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.

    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school.

13. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider as soon as possible.

17. If I have lost any school/setting related documents or files, I will report this to the ICT Support Provider and school Data Protection Officer as soon as possible.

18. Any images or videos of learners will only be used as stated in the school camera and image use policy.
    - I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

19. I am aware of safe technology use in the classroom, safe remote learning, and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.

20. I have read and understood the school online safety policy which covers expectations for learners regarding mobile technology and social media.

21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.
    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) Emma Law or a deputy as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the school online safety/child protection policy.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

24. I have read and understood the school online safety policy which covers expectations regarding staff use of mobile technology and social media.

25. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    - I will take appropriate steps to protect myself online when using social media as outlined in the online safety policy
    - I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety policy.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school code of conduct and the law.

26. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels, such as a school email address or telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
    - If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or Headteacher.

27. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the Headteacher.

28. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

29. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

30. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Compliance

31. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

32. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school online safety policy.

33. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the allegations against staff policy.

34. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

35. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

36. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with East Stour Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……………………………………………………………………………………

Signed: ………

Date (DDMMYY)……………………………………………………...

Visitor and Volunteer Acceptable Use of Technology Policy

For visitors and volunteers (and staff) who do not have access school/setting ICT systems.

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This AUP will help East Stour ensure that all visitors and volunteers understand the school expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within East Stour both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage and communication technologies.

2. I understand that East Stour AUP should be read and followed in line with the school staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. Any images or videos of learners will only be taken in line with the school camera and image use policy

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.

7. Where I deliver or support remote learning, I will comply with the school remote learning AUP and protocols.

8. I will support teachers in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the Designated Safeguarding Lead (DSL) in line with the school online safety policy.

10. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music is protected, I will not copy, share or distribute or use it.

Use of Social Media and Mobile Technology

11. I have read and understood the school online safety policy which covers expectations regarding staff use of social media and mobile technology.

12. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the online safety/social media policy.
    - I will not discuss or share data or information relating to learners, staff, school/setting business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct and the law.

13. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL.

14. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead

15. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

16. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

17. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Breaches or Concerns

18. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the school online safety/child protection policy.

20. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the allegations against staff policy.

21. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

22. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with East Stour visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ………………………………………………………………………………………

Signed: ………

Date (DDMMYY)…………………………………………………...

Wi-Fi Acceptable Use Policy

For those using setting provided Wi-Fi. Settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. This template is provided for settings to adapt and use as appropriate.

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The school provides Wi-Fi for the school community and allows access for education use only

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school

3. The use of technology falls under East Stour Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School/ owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

12. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead.

16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with East Stour Wi-Fi acceptable Use Policy.

Name ………………………………………………………………………………...

Signed: …………………………………………………………………….Date (DDMMYY)………………

Template Acceptable Use Policy (AUP) for Remote Learning and Online Communication

These templates specifically address safer practice when running formal remote learning, including live streamed sessions, but can also apply to other online communication, such as remote parent meetings or pastoral activities. There is no expectation that staff should run formal live streamed sessions or provide pre-recorded videos; settings should implement the approaches that best suit the needs of their community and staff following appropriate discussions.

This content can either be used to create a standalone AUP or can be integrated into existing documents according to setting preference.

A remote learning AUP should be completed following a thorough evaluation of remote learning tools with approval from leadership staff. We recommend settings use existing systems and/or education focused platforms where possible, and that staff only use approved accounts and services to communicate with learners and/or parents/carers.

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
  - Kelsi: Guidance for Full Opening in September
    - Online Safety Guidance for the Full Opening of Schools
  - The Education People:' Safer remote learning during Covid-19: Information for School Leaders and DSLs'

- National guidance:
  - DfE 'Safeguarding and remote education during coronavirus (COVID-19)
  - SWGfL: Safer Remote Learning
  - LGfL: Coronavirus Safeguarding Guidance
  - NSPCC: Undertaking remote teaching safely
  - Safer Recruitment Consortium: 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020

Remote Learning AUP Template - Staff Statements

Supply staff or online tutors employed by the school/setting should agree and follow your child protection policy, staff behaviour policy and associated AUPs.

East Stour Primary School Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of East Stour community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using SeeSaw
   - SeeSaw has been assessed and approved by the Senior Leadership Team (SLT).
2. Staff will only use school managed or specific, approved professional accounts with learners and/or parents/carers.
   - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
     - o Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Emma Law, Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device. If this is not available then expectations are in place in relation to safeguarding and data security when using personal devices e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.
3. Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT:
   - 8.30am-4.00pm.
4. All remote lessons will be pre recorded.
5. Live streamed remote learning sessions will only be held with approval and agreement from the headteacher/a member of SLT and only when the children are in school and the adult is isolating at home.

Data Protection and Security

6. Any personal data used by staff and captured by SeeSaw when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
   (The school continue to follow the guidance outlined in the data protection: toolkit for schools when managing personal data)
7. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the remote learning policies and procedures.
8. All participants will be made aware that SeeSaw keeps record of activity..
9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
10. Only members of the East Stour community will be given access to SeeSaw.
11. Access to SeeSaw will be managed in line with current IT security expectations as outlined in the GDPR policy.

- Privacy expectations remain the same e.g. using strong passwords, logging off or locking devices when not in use etc.

Session Management

12. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Pre-recorded sessions or only live links when the children are in school and another adults overseeing the class.
13. When live streaming with learners:
    - contact will be made via staff in school's email accounts
    - another member of staff will be present.
14. A pre-agreed email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Staff should not forward or share access links.
    - Learners are encouraged to attend lessons in a classroom when appropriately supervised by an appropriate school adult.

Behaviour Expectations

15. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
16. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
17. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
18. When sharing videos participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
19. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

20. Participants are encouraged to report concerns during remote and/or live streamed sessions to their class adult.
21. If inappropriate language or behaviour takes place the member of staff will use the school's behaviour systems.
22. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
23. Any safeguarding concerns will be reported to Emma Law Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the East Stour Primary School Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……………………………………………………………………

Date……………………………

Remote Learning AUP Template - Learner Statements

East Stour Primary School Learner Remote Learning AUP

I understand that:

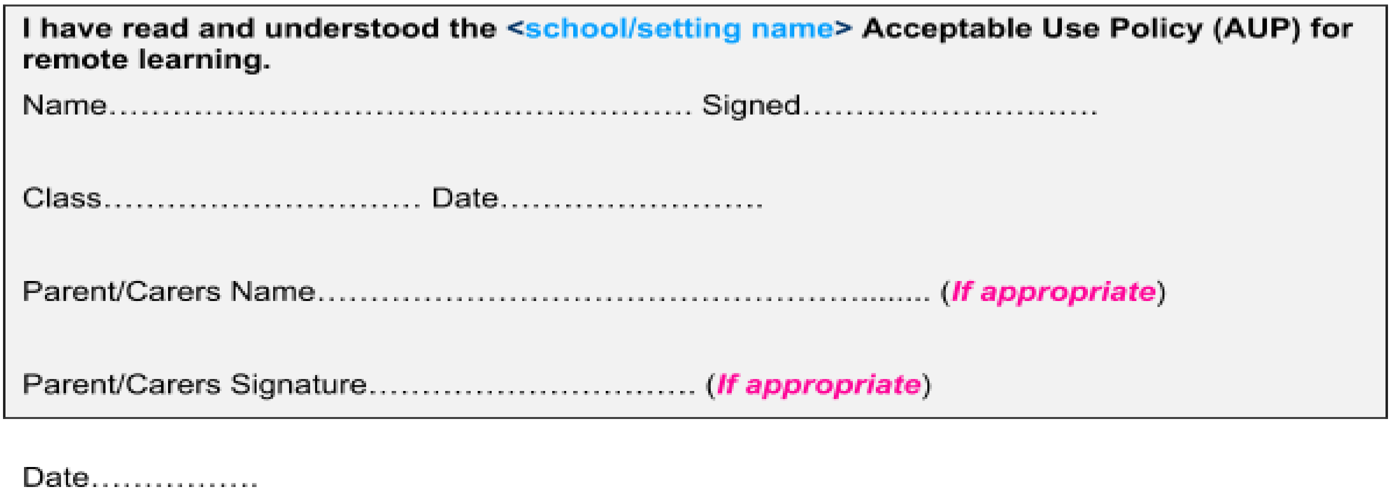
- these expectations are in place to help keep me safe when I am learning at home using SeeSaw
- I should read and talk about these rules with my parents/carers.
- remote learning will only take place using SeeSaw and during usual school times.
- My use of system name is monitored to help keep me safe.

2. Only members of East Stour community can access SeeSaw
    - I will only use my school provided login to access remote learning.
    - I will use privacy settings as set up by the school.
    - I will not share my login/password with others
    - I will not share any access links to remote learning sessions with others.

3. When taking part in remote learning I will behave as I would in the classroom. This includes:
    - Using appropriate language.
    - Not taking or recording images/content without agreement from the teacher and/or those featured.

4. If I am concerned about anything that takes place during remote learning, I will:
    - Report concerns to the members of staff from my class or tell a parent/carer

5. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:
    - The school restricting/removing access, informing parents/carers, contacting police if a criminal offence has been committed.



I have read and understood the <school/setting name> Acceptable Use Policy (AUP) for remote learning.

Name.. Signed.............................

Class.............................. Date.........................

Parent/Carers Name.. (***If appropriate***)

Parent/Carers Signature................................ (***If appropriate***)

Date................

Acknowledgements and Thanks

These statements have been produced by The Education People Education Safeguarding Service.

Additional thanks to members of the Kent Education Online Safety Strategy Group, the UK Safer Internet Centre, South West Grid for Learning (SWGfL), London Grid for Learning (LGfL), South East Grid for Learning (SEGfL), Childnet , CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.