Staplehurst School
Online Safety Policy

Policy reviewed by the Online Safety Group	October 2020
Policy approved by the **Full Governing Body**	24 November 2020
Policy to be next reviewed	Autumn Term 2023

Designated Members of Staff

The Designated Safeguarding Lead (DSL) is Lucy Davenport, Headteacher.

Contact details: Tel 01580 891765 or Ldavenport@staplehurst.kent.sch.uk

The DSL is supported by Deputy DSLs:

- Vicky French, Assistant Head for Inclusion
- Bonny Sullivan, Family Liaison Manager
- Lloyd Williams-Jones, Deputy Head

The Link Governor for Safeguarding is **Caroline Bennett**, Parent Governor, clerktogovernors@staplehurst.kent.sch.uk

The School's Online Safety group consists of the following members:
Vicky French (Chair and Assistant Head Inclusion),
Sarah Beecham (ICT Technician),
Caroline Bennett (Safeguarding Link Governor and Parent),
Leanne Carter (Parent),
Nusrat Wahid (Admin and Social Media),
Jack Tate (DPO and KS2 Lead)
Lisa Carrie (Clerk)

Contents

Online Safety Policy

1. Policy Aims

- This Online Safety policy has been written by Staplehurst School, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) Online Safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2018, Early Years and Foundation Stage 2017 Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Board (KSCB) procedures.
- The purpose of Staplehurst School Online Safety policy is to:
  - Safeguard and protect all members of Staplehurst School community online.
  - Identify approaches to educate and raise awareness of Online Safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to Online Safety concerns.
- Staplehurst School 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

- Staplehurst School believes that Online Safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Staplehurst School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Staplehurst School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- 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 school (collectively referred to as 'Staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Staff Acceptable Use Policies (AUP) and Staff Code of conduct
  - Behaviour and Discipline (including anti-bullying) policy
  - Safeguarding (including Child protection) policy
  - Confidentiality policy
  - Data Protection policy
  - Curriculum policies, such as: Computing Curriculum Plans, Spiritual, Moral, Social and Cultural (SMSC) policy which includes Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. The Online safety Group will review this policy three times per year and the Governing Body will review this policy at least annually. The policy will

also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

- We will ensure that we 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 a regular basis to the governing body on Online Safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) named at the front of this policy has lead responsibility for online safety.
- Staplehurst School 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:

- Ensure that Online Safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding Online Safety; including a Code of Conduct and/or an AUP, which covers Staff acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that Online Safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of Online Safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their Online Safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding Online Safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate Online Safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead[1] (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented
- Ensure all members of staff receive regular, up-to-date and appropriate Online Safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date 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
- Keep up-to-date with current research, legislation and trends regarding Online Safety (by attending external training events and review guidance documents released by relevant organisations) and communicate this with the school community, as appropriate..
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

[1] All references to DSL will be deemed to include deputy DSLs

- 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 schools safeguarding recording mechanisms.
- Monitor Online Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report Online Safety concerns, as appropriate, to the 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 at least three times per year with the Online Safety Group.
- Consult with pupils via the School Council as and when is appropriate

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

- Contribute to the development of Online Safety policies.
- Read and adhere to the Online Safety policy and AUPs.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and 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 children in their care.
- Identify Online Safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate Online Safety issues, including signposting 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 leadership team, especially in the development and implementation of appropriate Online Safety policies and procedures.
- Implement appropriate security measures *(*including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering and monitoring systems are applied and updated on a regular basis
- Ensure appropriate access and technical support is given to the DSL to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of pupils[2] to:

- Engage in age appropriate Online Safety education opportunities.
- Contribute to the development of Online Safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing Online Safety issues.

[2] at a level that is appropriate to their individual age, ability and vulnerabilities

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their Online Safety approaches by discussing Online Safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school Online Safety policies.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- To follow the school's complaints procedure if they wish to make a complaint at any time and not use social media to complain about the school, any of its staff or its pupils. The school will follow KCC's guidance on "Dealing With Complaints against Schools and Settings by Parents or Carers on Social Networking Sites" and will not tolerate and behaviour that could upset, offend or threaten the safety of any member of the school community.

4.7 It is the responsibility of visitors and members of the community:

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive Online Safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including Online Safety in the Computing and Spiritual, Moral, Social and Cultural (SMSC) Curriculum, covering use both at home school and home.
  - Reinforcing Online Safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology by pupils. The Computing Subject Leader is considering reintroducing the pupil Digital Leaders programme.
  - Implementing appropriate peer education approaches via the Student Council.
  - Providing Online Safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking pupil voice when writing and developing school Online Safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support the schools internal Online Safety education approaches.

5.1.1 Vulnerable Pupils

- Staplehurst School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Staplehurst School will ensure that differentiated and ability appropriate Online Safety education, access and support is provided to vulnerable pupils. The School uses Partners in Excellence (PiXL) resources
- Staplehurst School will seek input from specialist staff as appropriate, including the SENCO.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the Online Safety policy with all members of staff as part of induction, ensuring that they fully understand the school Online Safety policy and Staff ICT Acceptable Use Agreement (AUP) see Appendix 1.
- Provide up-to-date and appropriate Online Safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities in Staff Meetings for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding Online Safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

- Staplehurst School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school 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. This includes a dedicated Online Safety page on the school's website plus on virtual learning platforms, parent workshops and parents evenings, curriculum activities, letters and newsletters, social media alerts, workshops and high profile events e.g. Safer Internet Day. The website also has an anonymous reporting button.
  - Drawing their attention to the school Online Safety policy and expectations in newsletters, letters, and website.
  - Requesting that they read Online Safety information as part of joining our school, for example, within our home school agreement.
  - Requiring them to read the school AUP and discuss its implications with their children.
  - If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL
  - Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Reducing Online Risks

- Staplehurst School 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 use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

- All members of the school community are made aware of the school's 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 to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Staplehurst School uses a wide range of technology. This includes access to:
  - Computers, laptops, iPads and other digital devices
  - Internet which may include search engines and educational websites
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place e.g. Mobile Device Management (MDM).
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools e.g. Google Safe Search, following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1** - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
  - **Key Stage 2 -** Pupils will use age-appropriate search engines and online tools. Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All Staff [3]are responsible for ensuring that they have read and understood the Staff Acceptable Use Policy prior to use of the School's ICT systems – see Appendix 1 – the Staff ICT AUP will be included in the Staff Code of Conduct/Handbook
- The Pupil Acceptable Use Policy will be explained to all pupils prior to allowing access to the School's ICT systems - See Appendix 2
- All parents will be made aware of the Pupil Acceptable Use Policy via the Home School Agreement – see Appendix 3
- Supply teachers who attend school on a regular basis will be given their own login and required to set their own passwords. The School has a guest login for ad hoc supply teachers use - the password is reset regularly by the ICT technician.

[3] Including external contractors, visitors, volunteers and other individuals who are provided with access the school's ICT systems

- Governors Wi-Fi access is managed through governor specific access login.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Staplehurst School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's 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.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Internet access is managed through Cantium Business Solutions. The School uses educational filtered secure broadband connectivity through the Kent's Public Service Network (KPSN) which is appropriate to the age and requirement of our pupils. The network uses Smoothwall to block inappropriate sites.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list
- The network provides enhanced / differentiated user-level filtering and control access to social media and social networking sites.
- The School will work with Cantium and the Schools' Broadband team to ensure that filtering is continually reviewed.
- The Search Engine Bing, which has no equivalent of Google's SafeSearch, is blocked automatically at firewall.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
  - If pupils discover unsuitable sites, they will be required to follow the "Bother actions" detailed in Appendix 5
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is managed by Cantium.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. The DSL will respond in line with the School's Safeguarding or managing allegations policies.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the General Data Protection Regulations and associated data protection legislation
- Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a Data Protection Impact Assessment (DPIA) must be carried out to assess:
    - whether the processing is necessary and proportionate in relation to its purpose
    - the risks to individuals
    - what measures can be put in place to address those risks and protect personal information.

Full information can be found in the schools **Data Protection policy.**

7.5 Security and Management of Information Systems

- Internet security is managed through Cantium
- The school takes appropriate steps to ensure the security of our information systems, including:
    - The School infrastructure and individual workstations are protected by anti-virus software, which is 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.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments. Software is to be approved by the ICT Technician and may only be installed by the ICT Technician or the managed IT service provider. Software is not permitted to be transferred via email attachment.
    - Staff are not permitted to download executable files and install programmes on School devices unless otherwise agreed by the ICT Technician
    - Regularly checking files held on the school's network,
    - The appropriate use of user logins and passwords to access the school network.
    - All users are expected to log off or lock their screens/devices if systems are unattended. Equipment will be secure and if necessary locked away when not in use.
    - An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
    - Users are not permitted to use School devices inside or out of school for personal use.
    - Any personal data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the School. Only the School's removable media (e.g. memory sticks / CDs / DVDs) are to be used on the School's ICT system unless specifically agreed by the ICT Technician.
    - Contact details published on the School website will be limited to the School address, main telephone number and fax number.
    - Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From year 1, pupils are provided with their own unique username. A tiered password protocol is being developed for pupils.
- The " administrator" passwords for the School ICT systems, Incident Report Tool and voice & video internet platform accounts, used by the ICT Technician must also be available to the Headteacher and kept in the School safe.
    - They are also kept securely (password protected) on the network.
    - An audit is carried out once a year to ensure this information is kept up to date.
- We require all users (other than pupils) to:
    - Use strong passwords for access into our system.

- Change their passwords regularly
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school 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 pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the school's **Digital Images, Video & Media Agreement** Appendix 4.

7.8 Managing Email

- Access to school email systems will always take place in accordance with data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
  - 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.
  - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications. Staff official blogs or wikis should be password protected and run from the School website.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

- Currently pupils are not provided with individual email accounts but, if deemed appropriate in the future for educational purposes:
  - upper KS2 pupils may be allocated an individual school email address, and,
  - other pupils may use whole-class or group email addresses,

  for communication outside of the school.
- Pupils will be made aware of the AUP and will receive education regarding safe and appropriate email etiquette before such access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- Videoconferencing and/or Webcams **are only used with the prior agreement of the Headteacher.**

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities - See Digital Images, Video & Media Agreement in Appendix 4.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message. Such communications will be supervised appropriately for the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- 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, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.9.3 Videoconferencing Safeguarding Protocol

- When videoconferencing sessions take place, pupils, parents and staff must be made aware of and adhere to the following expectations.
    1. A parent or guardian must be in the room when the child is participating in a videoconference e.g. ZOOM meeting. Children are not to be left unsupervised.
    2. Staff and children must wear suitable clothing, as should anyone else in the household.
    3. Recording devices used should be in appropriate areas e.g not bathrooms or bedrooms.
    4. Language must be professional and appropriate, including any family members in the background.
    5. Videos may be muted for both pupils and staff if other children in the household become unsettled or cause a disruption.
    6. Screenshots of the meeting must not be taken or shared.

    - Failure to follow these expectations may result in your being forced to leave the meeting.
    - By allowing your child to join the meeting, you give consent and accept the above terms.

- When videoconferencing sessions take place, staff must be made aware of and adhere to the following expectations.
    1. Staff must use a school email account to log into ZOOM.
    2. Each meeting must be booked with a separate password (not recurring) to be shared with parents via the appropriate year group email account.
    3. Waiting Room facility must be engaged and waiting room locked when meeting begins.
    4. Meeting must be recorded via ZOOM recording facility and ensure participants are aware. The recording must be saved to the school system.
    5. Call must be logged on the call log sheet.
    6. No 1:1 meetings should take place, group only.
    7. Screen sharing must only take place from the school network.

7.10 Management of Applications

- Staplehurst School uses a number of Online Applications (Apps) for pupil learning and recording pupil progress.
    - Learning Apps e.g. MyMaths, Times Table Rock Stars, and Spelling Shed.
    - Recording Pupil Progress - Target Tracker & PiXL
    - The school is considering using Tapestry for recording Early Years pupil data in the future.
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation including the GDPR and associated data protection legislation.
- To safeguard pupil's data:
    - Only school 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 pupils' 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 Staplehurst School 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 Staplehurst School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of Staplehurst School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
    - The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - Inappropriate use of social media on school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Staplehurst School community on social media, should be reported to the school and will be managed in accordance with our **Behaviour & Discipline, Allegations against staff, and Safeguarding policies.**
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the site's terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing 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 the School Code of Conduct and the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. 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 the privacy levels of their personal sites as strictly as they can.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Staplehurst School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also 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 and to ensure that their social media use is compatible with their professional role and is in accordance with schools 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 pupils 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 in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with the Headteacher.
  - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools DSL.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be

raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

- Pupils will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
  - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
  - Not to meet any online friends without a parent/carer or other responsible adult's permission and only 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 and report concerns both within school and externally. Pupils should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately and safely when using digital technologies

8.4.1 Official Use of Social Media

- The school official social media channels are Facebook and Twitter.
- **The school will not share any staff or pupil personal data on the official Facebook or Twitter pages**.
- **Digital images will not be shared without parental consent**.
- The official use of Facebook and Twitter only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The use of Facebook and Twitter as communication tools has been formally risk assessed and approved by the Headteacher.
  - Leadership staff have access to account information and login details for our Facebook and Twitter pages, in case of emergency, such as staff absence.
- The school's official Facebook and Twitter pages have been set up as distinct and dedicated account for educational or engagement purposes only.
  - Staff use the school provided email addresses to register for and manage the page.
  - Public communications on behalf of the school will be restricted to authorised staff only, and where appropriate and possible, be read and agreed by at least one other colleague.
- Official Facebook and Twitter use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms 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.
- We will ensure that any official Facebook or Twitter use does not exclude members of the community who are unable or unwilling to use these channels.

Staff expectations

- Members of staff who follow and/or like our official social media profiles 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 school, they will:
  - Sign our acceptable use policy.
  - Always be professional and aware they are an ambassador for the school.
  - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the school.

- Always be 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.
- Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform the Headteacher and/or the DSL of any concerns, such as criticism, inappropriate content or contact from learners.

9 Use of Personal Devices and Mobile Phones

- Staplehurst School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.
- Full guidance on use of personal devices and mobile phones can be found in the school's Mobile Phone Policy.

10 Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for Online Safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
  - In the event of an Online Safety incident or concern all Users must tepee the laptop or turn off the monitor and report the incident in accordance with the School's "Bother Actions" - see Appendix 5.
  - All Online Safety incidents/concerns (including but are not limited to accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites) must be reported immediately to DSL using "Green Form" as detailed in the School's Safeguarding policy
  - All Users must report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
  - Parents/Carers and local community groups and members may report Online Safety incidents/concerns by email to the DSL or via the School's website through the anonymous reporting app
  - If the school is unsure how to proceed with an incident or concern, the DSL will refer to KCC's Responding to an Online Safety Concern Flowchart and will seek advice from the Education Safeguarding Team.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure
- The school requires staff, parents, carers and pupils to work in partnership to resolve Online Safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any Online Safety incidents involving safeguarding or child protection concerns. The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that Online Safety concerns are escalated and reported to relevant agencies in line with the KSCB thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Managing Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
- Appropriate action will be taken in accordance with the Discipline policy and Code of conduct.

11 Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018

The school recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our **Safeguarding and Behaviour & Discipline policies.**
- The school recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment..
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

- Staplehurst School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the DSL.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Staplehurst School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative

approaches, via a range of age and ability appropriate educational methods recommended by KCC/ Childnet.

- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. In this case, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.
- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
  - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
  - Ensure the DSL responds in line with the guidance.
  - Store the device securely. If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Specialist Children's Services and/or the Police, as deemed appropriate in line with the guidance.
  - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with the school's **Behaviour & Discipline** policy, but taking care not to further traumatise victims where possible.
  - Consider the deletion of images in accordance with the guidance. Images will only be deleted once the school 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. 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 Child Sexual Abuse and Exploitation

- Staplehurst School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Staplehurst School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community on the School website.
- If the school are made aware of incident involving online sexual abuse of a child, the school will:
  - Act in accordance with the school's safeguarding policy and the relevant KSCB's procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Specialist Children's Services (if required/ appropriate) and immediately inform Kent police via 101 (or 999 if a child is at immediate risk)

- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
  - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report
- If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Staplehurst School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
  - Act in accordance with the schools child protection and safeguarding policy and the relevant KSCB's procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
  - Ensure that the DSL is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
  - Ensure that the DSL is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the Headteacher is informed in line with our Managing Allegations of Abuse against Staff policy.
  - Inform the LADO and other relevant organisations in accordance with the schools managing allegations 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 Staplehurst School.
- Full details of how the school will respond to cyberbullying are set out in the **Behaviour & Discipline policy.**

11.5.1 Cyberbullying Definition

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

11.5.2 Preventing and Addressing Cyber-Bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

11.5.3 Examining Electronic Devices

- School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
- When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
  - Cause harm, and/or
  - Disrupt teaching, and/or
  - Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
  - Delete that material, or
  - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
  - Report it to the police

- Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Staplehurst School and will be responded to in line with existing school's **Behaviour & Discipline policy.**
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.7 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with the **Safeguarding policy**.
- If the school is 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 school's policies.

12 Useful Links for Educational Settings

12.1 Kent Support and Guidance for Educational Settings

Education Safeguarding Team:

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

KSCB:

- 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 other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- Cantium - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.Cantiumkent.co.uk

12.2 National Links and Resources for Educational Settings

- CEOP:
- www.thinkuknow.co.uk
- www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org

- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

12.3 National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
- www.thinkuknow.co.uk
- www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Appendix 1 – Staff ICT Acceptable Use Policies

(To be signed by all Staff including governors, leadership team, teachers and support staff; and any external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school AND have access the school's ICT systems)

As a professional organisation with responsibility for safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the School's Information Communication Technology (ICT) system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using the School's ICT systems, they are asked to read and sign this Acceptable Use Policy (AUP).

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the School's ethos, other appropriate School policies, relevant national and local guidance and expectations, and the Law.

- I understand that ICT systems include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, tablets, mobile phones, digital cameras, email and social media sites**.**
    - School owned information systems must be used 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.
    - I understand that any hardware and software provided by the School for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended – I will lock my login or logout as appropriate. I will protect the devices in my care from unapproved access or theft.
- I will respect ICT system security and I will not disclose any password or security information. I will change my password at least termly. I will use a 'strong' password (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).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Technician.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with General Data Protection Regulations and associated data protection legalisation.
    - This means that 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 (only within countries or sites with suitable data protection controls) or accessed remotely e.g. Virtual Private Network (VPN).
    - Any data which is being removed from the School site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the ICT Technician.
    - Any images or videos of pupils will only be used as stated in the School's Online Safety policy and will always take into account parental consent.
- I will not keep professional documents which contain School-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones) or personal removable media (e.g. memory sticks / CDs / DVDs); unless I have permission from the DSL and the files are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment (if appropriate) or via VPN.
- I will not store any personal information on the School computer system (including any School laptop or similar device issued to members of staff) that is unrelated to School activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the School Online Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites, and the supervision of pupils within the classroom and other working spaces.

- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the DSL as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the School. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any School related documents or files, then I will report this to the DSL and DPO as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times.
    - All communication will take place via School approved communication channels e.g. via a School provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher
- I will ensure that my online reputation and use of ICT systems are compatible with my professional role, whether using School or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
    - I will take appropriate steps to protect myself online as outline in the Online Safety policy and will ensure that my use of ICT systems will not undermine my professional role, interfere with my work duties and will be in accordance with the School's Code of Conduct and AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the School, or the County Council, into disrepute.

- I will promote Online Safety with the pupils 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.

- If I have any queries or questions regarding safe and professional practise online either in School or off site, then I will raise them with the DSL, or in their absence the Headteacher.
- I understand that my use of the school information systems, including any devices provided by the school, school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
- I understand that the school may exercise its right to monitor the use of ~~i~~nformation systems, including internet access and the interception of emails. Where it believes unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

- **I have read, understood and agree to comply with Staplehurst School Staff Acceptable Use Policy**

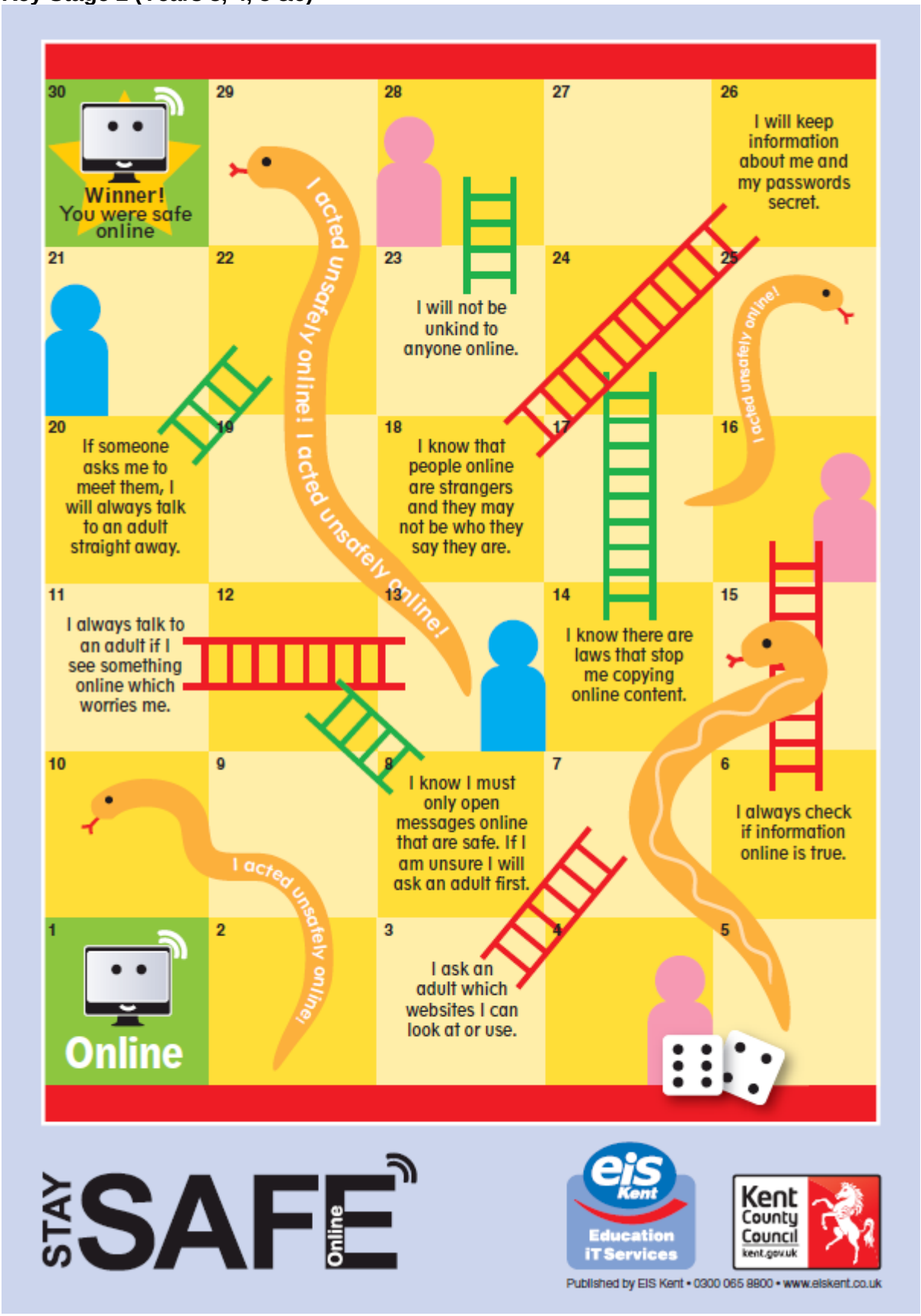
- Name: …… Signed: ……..... Date: ……

- Accepted by: …… Date: ……

Appendix 2 – Pupil Acceptable Use Policy

Early Years and Key Stage 1 (Years 1 & 2)

Key Stage 2 (Years 3, 4, 5 &6)



Appendix 3 - Home School Agreement

The School's Values
Staplehurst is a school that is happy, purposeful and stimulating where each child's needs are viewed individually, by a staff of highly trained classroom practitioners who demonstrate excellence underpinned by high expectations and professionalism.

Our aim is to instil, in each unique pupil, a love of learning; develop their confidence in order to reach their full potential; and cultivate the lifelong skills of independence, creative thinking, team work and effective participation.

We all agree to live by our school values of:

Pride, Positivity, Respect, Integrity, Determination and Excellence

School's Responsibilities
It is the responsibility of the School:

- To safeguard and promote the welfare of all children who are pupils at a school
- To provide a balanced curriculum and meet the individual needs of its pupils
- To promote pupils' spiritual, moral, social and cultural development, including promoting fundamental British values of democracy, the rule of law, individual liberty, and mutual respect and tolerance of those with different faiths and beliefs.

Parents/Carers Responsibilities
It is the responsibility of the parents/carers:

- To respect and support the School's values
- To take an active interest in their child's education, to encourage him/her to stretch themselves and provide the support and environment to maximize their academic potential.
- To encourage their child to take as full and active part in school life as possible.
- To support the School and its policies, particularly in respect of safeguarding (including online safety), attendance, behaviour, and homework
- To understand the School's duty to take action if a pupil's behaviour onsite, offsite and/or on-line adversely affects the wellbeing of other pupils and support the School's actions in response to such issues
- To understand the School's responsibilities to safeguard pupils and support the School's actions; in particular driving and parking safely in the vicinity of the School's gates at all times.
- To support the School's online safety policy by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing Online Safety with them when they access technology at home. And not using social media to upload or share photos that contain any pupil other than their own child(ren).
- To follow the school's Complaints Procedure if they wish to make a complaint at any time and not use social media to complain about the school, any of its staff or its pupils.

Pupil's Responsibilities
It is the responsibility of the pupil:

- To respect and support the School's values
- To work to the best of their abilities at all times including homework
- To take a full part in school life
- To follow the school rules and treat the school community with respect at all times including onsite, offsite and on-line.

Please read and sign this agreement and return to the class teacher. Please complete one Agreement per child. This Agreement will remain in place for your child's duration at the school.
Pupil Name _____
We agree to work together to help the above pupil to achieve real success in fulfilment of their potential and making a contribution to the life of the School.
Parent/Carer signature: _____ ***Date:*** _____

Pupil's signature: _____ ***Date:*** _____

Appendix 4 – Digital Images, Video & Media Agreement

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, parents / carers and pupils need to be aware of the risks associated with publishing images on the internet. The School will implement the following procedure to reduce the likelihood of the potential for harm:

- When using images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular pupils should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take images to support educational aims, but those images should only be taken on School equipment.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Care should be taken when taking images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Images published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' first names only will be used on a website or blog, particularly in association with images.
- Images published in the press will not include pupils' names.
- Pupils' first names only will be used on the School Newsletter.
- Parents/carers are welcome to take images of their children at School events for their own personal use but the School requests these are NOT posted online.

✂ ----------

Digital Images, Video and Media Agreement

Please see the School's Privacy Notice on the website for information about how we use and may share personal data.

I will support the School and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I agree to digital images/video of my child & my child's work being published in school literature and in public displays, on the school's ICT systems (including website or voice & video internet platforms etc). (*delete if not applicable*)

I agree to digital images/video of my child & my child's work being published in the press (including on TV, or being included in radio programmes) in connection with school issues. (*delete if not applicable*)

Signed_____ Date _____

Parent of _____ Class _____

Appendix 5 – Pupil Incident Reporting (Bother Actions)

eSafety
Bother Actions

If something 'bothers' me online,
I 'bother' to do something about it!!
At School or At Home

Actions

1. Laptop Tepee or Monitor Off
2. Tell an Adult
   or
   Use the Whisper Button
3. An Adult will Log
   and
   Respond to your 'Bother'