Staplehurst School
E-Safety (Online and Internet) Policy

Policy reviewed and ratified at a meeting of the **Full Governing Body** 15 March 2017

Policy to be next reviewed Autumn Term 2017

Designated Members of Staff

The Designated Safeguarding Lead (DSL), who has overall responsibility for Safeguarding, is **Katie Murray**, Inclusion Manager. Contact details: tel. 01580 891765 or kmurray@staplehurst.kent.sch.uk

In her absence these matters will be dealt with by **Cathy Farthing**, Headteacher. Contact details: tel. 01580 891765 or headteacher@staplehurst.kent.sch.uk

The E-Safety Officer is Kate Murray, Inclusion Manager. Contact details as above.

The Link Governor for Safeguarding (including e-safety) is:

Caroline Bennett, Parent Governor, clerktogovernors@staplehurst.kent.sch.uk

Contents

E-Safety Core Policy

Introduction

This E-Safety policy has been written by the E-Safety Group, building on the South West Grid for Learning (SWGfL) E-Safety Policy, the Kent County Council (KCC) E-Safety Policy and government guidance. This Policy must be read in conjunction with the School's E-Safety Policy Schedule (hereafter called the Schedule) which contains detailed procedures relating to the School's implementation of the E-Safety Policy.

Policy Statements

The Governing Body and staff of Staplehurst School take seriously our responsibility to safeguard and promote the welfare of our pupils, to minimise risk and to work together with other agencies to ensure adequate arrangements are in place within our school to identify, assess, and support those children who are suffering harm. The guiding principle of this e-safety policy is safeguarding pupils and this Policy should be read in conjunction with the School's Safeguarding policies.

The purpose of the School's Information Communication Technology (ICT) system is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.

ICT systems are an essential element in everyday life for education, business and social interaction. The School has a duty to provide pupils with a quality ICT system in order to provide an appropriate environment for their learning experience. ICT System use is part of the statutory curriculum and is a necessary tool for learning.

Pupils use ICT systems widely outside School and so need to learn how to evaluate information and to take care of their own safety and security. Pupil instruction regarding responsible and safe use of ICT systems will precede access. Safe and responsible use of ICT systems will be reinforced across the curriculum and subject areas.

Use of the School's ICT system is an entitlement for pupils who show a responsible and mature approach to its use. All users will have clearly defined access rights to the School's ICT systems. These access levels will be reviewed to reflect curriculum requirements and the age and ability of pupils.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the School's E-Safety provision. Children and young people need the help and support of the School to recognise and avoid E-Safety risks and build their resilience.

The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of ICT systems, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. Neither the School nor KCC can accept liability for the material accessed, or any consequences resulting from ICT system use.

Scope of the Policy

The E-Safety Policy applies to all members of the School community (including governors, staff, contractors, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of School ICT systems, both in and out of the School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the School, but is linked to membership of the School.

The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

Safeguarding

The E-Safety Group, DSL and leadership team have read and will follow the guidance detailed in Annex C of the DfE's Keeping Children Safe in Education September 2016 Guidance regarding Online Safety.

The School will ensure that all members of the community are made aware of:

- The social, psychological and criminal consequences of sharing, possessing and creating incident images of children including self-generated indecent images **e.g. sexting**
- Online child sexual abuse, including **exploitation and grooming** including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. Definitions and signs and symptoms of such abuse are detailed in the School's Safeguarding policy.

The School has a statutory duty to have due regard to the need to **PREVENT** people from the **risk of radicalisation.** The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.

All concerns will be reported to and dealt with by the DSL. For more information on the School's Safeguarding reporting procedures please refer to the School's Safeguarding Policy.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the School:

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about E-Safety incidents and monitoring reports from the E-Safety Link Governor.
- The role of the E-Safety Governor will include: regular meetings with the E-Safety Officer and Technician, regular monitoring of E-Safety incident log and implementation of the E-Safety policy and reporting to the relevant Governing Body sub-committee.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the School community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Officer.
- The Headteacher and (at least) another member of the Senior Leadership should be aware of the policy to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- To ensure that the Designated Safeguarding Lead (DSL), SENCo and e-Safety Officer work in partnership on e-Safety matters if they are not the same individual

E-Safety Officer:

- The E-Safety Officer takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the School's E-Safety policies, procedures and documents. They lead the E-Safety Group and liaise with the Local Authority and School technical staff.
- The E-Safety officer also ensures that all staff are aware of the procedures detailed in the Schedule and provides training and advice for staff.
- The E-Safety officer is responsible for receiving reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments. They meet regularly with the E-Safety Link Governor to discuss current issues, review incident logs, report regularly to the Senior Leadership Team and if requested attend relevant Governor meetings.

E-Safety Technician:

The E-Safety Technician is responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- that the School meets required E-Safety technical requirements and any Local Authority (or other relevant body) E-Safety policy or guidance that may apply.
- that users may only access the networks and devices through a properly enforced Access Procedure as detailed in the Schedule
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the School's ICT system is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Officer for investigation, action and/or sanction

Teaching and Support Staff

(Including but not limited to supply and trainee teachers, outside agencies staff, work experience staff, parent helpers or any other person who might use the School's ICT system for curriculum purposes)

Teaching and Support Staff are responsible for ensuring that they have an up to date awareness of E-Safety matters and of the School's E-Safety Policy and they have read and understood the Staff Acceptable Use Policy (AUP)

Teaching and Support Staff must also ensure that:

- they report any suspected misuse or problem to the E-Safety Officer for investigation, action and/or sanction
- E-Safety issues are embedded in all aspects of the curriculum and other activities and pupils understand and follow the E-Safety and acceptable use policies and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies and mobile devices in lessons and other School activities (where allowed) and implement current policies with regard to these devices

Designated Safeguarding Lead (DSL)

The DSL should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the School community, with responsibility for issues regarding E-Safety as detailed in the Schedule and the monitoring the E-Safety policy including the impact of initiatives.

Pupils:

- Pupils are responsible for using the School ICT system in accordance with the Pupil Acceptable Use Policy (AUP); and will be expected to know and understand policies on the use of personal devices. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Pupils must have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so and should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.

Parents/Carers

- Parents/Carers play a crucial role in ensuring that their children understand the need to use ICT systems in an appropriate way. A partnership approach to E-Safety at home and at school with Parents/Carers will be encouraged; they will be encouraged to support the School in promoting good E-Safety practice.

- Parents/Carers will also be encouraged to follow the School's guidelines on the appropriate use of digital images and video. They will be requested to sign the Digital Images, Video and Media Agreement.
- All Other Users (Including but not limited to community users and visitors not otherwise detailed above) who access the School's ICT systems as part of the wider School provision will be expected to sign Acceptable User Policy (AUP) before being provided with access to School systems.

Education and Training

It is essential that all users understand their responsibilities detailed above. The School will provide education and training as detailed in the Schedule.

ICT System

The School will be responsible for ensuring that the School's ICT system is as safe and secure as is reasonably possible and that all Access, Communication and Reporting procedures detailed in the Schedule are implemented. It will also need to ensure that the relevant people named in the Schedule will be effective in carrying out their E-Safety responsibilities.

The School's ICT system will be designed to enhance and extend education. The ICT system at the School will be managed to ensure that the School meets all recommended technical requirements and there will be regular reviews and audits of the safety and security of School ICT system.

Personal Devices on School Premises

The School does not currently operate a Bring Your Own Device (BYOD) programme. Pupils, Staff and Visitors are not permitted to bring personal devices onto School premises except to the extent detailed in the Schedule.

Personal devices of all kinds that are brought into School are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

Use of digital and video images

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images. The School's policy on the use of digital and video image is detailed in the Schedule.

Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with the School's Data Protection Policy.

Communications

The official School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored and staff and pupils should therefore use only the School email service to communicate with others when in School, or on School ICT system (e.g. by remote access). The School's Communication Procedure is detailed in the Schedule.

All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory The sending of abusive or inappropriate messages or content via any device is forbidden by any member of the School community and any breaches will be dealt with as part of the School's behaviour and discipline policies.

Users must immediately 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. The School's Reporting Procedure is detailed in the Schedule.

Social Media - Protecting Professional Identify

All Schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the

grounds of sex, race or disability or who defame a third party may render the School (or Local Authority) liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

All members of staff will be made aware that their online conduct out of School could have an impact on their role and reputation within School. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

The School provides the measures detailed in the Schedule to ensure reasonable steps are in place to minimise risk of harm to Pupils, Staff and the School.

Unsuitable and/or inappropriate activities

Some activities are unsuitable and/or inappropriate in a School context and Users should not engage in these activities in School or outside School when using the School ICT systems. Such activities are detailed in the Schedule. Any breaches will be dealt with as part of the School's behaviour and discipline policies.

Responding to incidents of misuse

In the event of suspicion of infringement of the E-Safety Policy all steps in the Procedure detailed in the Schedule should be followed.

The E-Safety Officer will record all incidents and actions taken in the School E-Safety Incident Log as well as any other relevant areas (e.g. Bullying or Child Protection) recording procedure.

After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will escalate the concern in conjunction with the School's Safeguarding policy and the will be reported to appropriate agencies such as Kent Police, Child Exploitation & Online Protection (CEOP) and/or Internet Watch Foundation (IWF) immediately.

School Actions & Sanctions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the School community are aware that incidents have been dealt with. The School will manage infringement of the E-Safety policy in accordance with the School's behaviour and discipline policies where appropriate

Complaints

Complaints about E-Safety will be dealt with under the School's Complaints Procedure. Any complaint about staff infringement of the E-Safety policy will be referred to the Headteacher. All E-Safety complaints will be also be recorded by the E-Safety Officer in the Incident Log, including any actions taken.

Monitoring and Review

The whole school community will have access a copy of this policy and will have the opportunity to consider and discuss its contents prior to the approval of the Governing Body being formally sought.

The implementation of this E-Safety policy will be monitored by the E-Safety Group. Monitoring will take place regularly. The E-Safety Group will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of pupils, parents/carers and staff.

The Full Governing Body will receive a report on the implementation of the E-Safety policy generated by the Safeguarding Link Governor as part of her termly report.

The Policy will be reviewed by the Governing Body every three years and the Schedule will be formally reviewed by the E-Safety Group annually; or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.

E-Safety Policy Schedule

Introduction

This Schedule forms part of the E-Safety Policy (hereafter called the Policy). It provides detailed procedural information relating the use of the School's Information Communication Technology (ICT) system and implementation of the E-Safety Policy and should be read in conjunction with the Policy itself.

E-Safety Group

The School's E-Safety group consists of the following members:

- E-Safety Officer – Katie Murray, Inclusion Manager & member of the Senior Leadership Team
- Staff – Fran Zimber, Business Manager and Sarah Beecham, ICT Technician
- Governors – Caroline Bennett, Safeguarding Link Governor (including E-Safety)
- Parents and Carers – Victoria Laslett
- Pupils (Digital Leaders) included as and when is appropriate

Members of the E-Safety Group will assist the E-Safety Officer with:

- the production, review and monitoring of the School E-Safety policy and supporting documents.
- the review and monitoring of the internet filtering and security service provided by Education IT Services (EiS)
- monitoring incident log
- consulting stakeholders – including parents and carers and the pupils about the E-Safety provision
- monitoring improvement actions identified through use of the KCC self-review tool

Education Provision

The School's website provides E-Safety information for the wider school community (this includes but is not limited to an E-Safety Helpdesk with links to relevant websites and publications). The website also has an anonymous reporting app. In addition to this publically available information the School will provide the following education to specific user groups:

Pupils

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. The E-Safety provision is detailed in the School's Computing Curriculum Plans which are available on the Curriculum area of the School's website.

The School is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate e-Safety education is given, with input from the SENCO as appropriate.

Staff

It is essential that all staff receive E-Safety training and understand their responsibilities as outlined in the Policy. Training will be offered as follows:

- A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Staff Acceptable Use Agreement (AUP) see Appendix 1.
- The E-Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.

Governors

Governors should take part in E-Safety training with particular importance for those who are members of any sub-committee involved in technology / E-Safety / health and safety / child protection.

Parents and/or Carers

Many parents/carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's on-line behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The School will take every opportunity to help parents understand these issues through curriculum activities, Letters and newsletters, workshops and high profile events / campaigns e.g. Safer Internet Day

The Wider Community

Currently the School shares its E-Safety knowledge and experience via its website. In the future the School may offer other learning opportunities to local community groups and members.

Access Procedure

Access to the School's ICT system is subject to the following procedures:

Acceptable Use Policies (AUP)

- All Staff 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 AUP will be included in the Staff 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 asked to sign the Home School Agreement – see Appendix 3
- The School is developing a procedure for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the School ICT system.

Passwords

- All users at KS2 and above will be provided with a username and secure password by the ICT Technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term for staff and biannually for pupils. KS1 pupils will also be assigned a username and password but they will not be required to change their password until they reach KS2.
- 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.

Software

- 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
- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Staff are not permitted to download executable files and install programmes on School devices unless otherwise agreed by the ICT Technician.

Internet Access (Filtering)

- Internet access is managed through Education IT Services EiS 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 School will work with EiS and the Schools' Broadband team to ensure that filtering is continually reviewed. There is a clear process in place to deal with the discovery of unsuitable sites and requests for filtering changes. Such requests will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- The School will control access to social media and social networking sites
- Staff who manage the filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and the Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- The School has provided enhanced / differentiated user-level filtering

Monitoring and Security

- School technical staff can access an activity report through EiS s and users are made aware of this in the Acceptable Use Agreement.
- Internet security is managed through EiS
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- The School infrastructure and individual workstations are protected by up to date virus software, which is updated regularly.
- 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.
- The ICT Technician will review system capacity regularly.
- Contact details published on the School website will be limited to the School address, main telephone number and fax number. Voice over IP (VoIP) contact information will not be put on the School website
- Equipment connected to the educational broadband network should 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
- Equipment will be secure and if necessary locked away when not in use.

Communications Procedure

All Communications are subject to the following procedures:

Email

- 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.
- Whole-class or group email addresses will be used in order to facilitate pupil communication with members outside of School. Any email sent from these accounts, must be approved by the pupil's class-teacher before sending. Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual School email addresses for educational use.

Social Media

- 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.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of School) will be raised with their parents/carers, particularly when concerning students' underage use of sites. 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.
- Pupils will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. They will be encouraged to approve and invite known friends only on social networking sites and deny access to others by making profiles private.

Voice & Video internet platforms (VoIP & Video Chat platforms)

(Including but not limited to Skype, YouTube and Google)

- Pupils will ask permission from a teacher before making or answering internet calls. Such communications will be supervised appropriately for the pupils' age and ability. Consent will be obtained from parents/carers prior to the children taking part in voice &/or video internet calls - See E-Safety Home School Agreement in Appendix 3.
- When recording a video for sharing on the School's website or voice & video internet platforms written permission will be obtained from all sites and participants. If third part materials are to be included in recorded video intellectual property rights must be checked to avoid infringements.
- All ICT devices within the School must be switched off when not in use and auto answer disabled. Webcams will be detached when not in use. Integral cameras and microphones will be masked when a device is in use outside of the learning environment to prevent unintentional or malicious recording.

Personal Information

Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

Personal Devices on School Premises

The School does not currently operate a Bring Your Own Device (BYOD) programme but Pupils, Staff and Visitors are permitted to bring personal devices onto the School premises subject to the conditions detailed below:

Pupils

- Personal devices are not permitted in the classroom and must be switched off then handed into the office at the beginning of the day for collection at the end of the day. Pupil's use of such devices during the day is not permitted unless prior arrangements have been made with a member of the Senior Leadership Team.
- If members of staff have an educational reason to allow children to use personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team
- Staff may confiscate or search a pupil's personal device and/or delete data, if they believe it is being used to contravene the School's behaviour policy. If there is suspicion that the material on the device may provide evidence relating to a criminal offence the device will be handed over to the police for further investigation.

Staff (excluding volunteer helpers)

- Staff are not permitted to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will be issued with a School phone where contact with pupils or parents/carers is required.
- Personal devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and personal devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team for use in emergency circumstances.

- Staff should **NOT** use personal devices to take digital images or videos of pupils and will only use work-provided equipment for this purpose Personal devices are not permitted in any circumstances to be used in certain areas within the School site such as changing rooms, toilets and swimming pools.

Visitors and Volunteer Helpers

Visitors and Volunteer Helpers are permitted to bring personal devices onto School premises but should not use such devices to take digital images or videos of pupils except to the extent permitted by the School's Digital Image and Video Sharing, Distribution and Publication Procedure detailed below.

Digital Image and Video Sharing, Distribution and Publication Procedure

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, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The School will inform and educate users about these risks and 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' full names will not be used anywhere on a website or blog, particularly in association with images.
- Written permission from parents/carers will be obtained and kept by the School before images of pupils or their work are published on the School's website or video sharing platform or in the press. Such permission will be retained by the School until the image is no longer in use. See Digital Images, Video & Media Agreement Appendix 4
- 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

Emerging Technologies

The table in Appendix 4 shows how the School uses emerging technologies. Use of such technologies is subject to the School's E-Safety procedures detailed in this Schedule. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

Protecting Professional Identify

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to Pupils, Staff and the School through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the School Acceptable Use Policy.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- A Technology Risk Assessment will be completed, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or School staff
- They do not engage in online discussion on personal matters relating to members of the School community
- Personal opinions should not be attributed to the School or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The School's use of social media for professional purposes will be checked regularly by the E-Safety Officer to ensure compliance with the Data Protection and Safeguarding Policies.

Unsuitable / inappropriate activities

The School believes that some activities are inappropriate in a School context and that users, should not engage in these activities in School or outside School when using School ICT systems. The School therefore restricts usage as detailed in Appendix 5.

Reporting Procedure

In the event of an E-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 6.

All E-Safety incidents/concerns (including but are not limited to accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites) must be reported immediately by email to the E-Safety Officer or via the School's website through the anonymous reporting app

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 E-Safety incidents/concerns by email to the E-Safety Officer or via the School's website through the anonymous reporting app

A dedicated email account will be set up for reporting wellbeing a pastoral issues, which will be managed by the E-Safety Officer

Responding to incidents of misuse

Upon receipt of an E-Safety incident report the E-Safety Officer (or in their absence senior member of staff) will follow the steps detailed in the navigation flow chart in the SWGfL online Incident Response Tool (IRT) www.boost.swgfl.org.uk (account login details are kept by the E-Safety Officer and stored in the School's safe for use by senior member of staff in their absence)

It is important that all of the steps in the online IRT are taken as they will provide an evidence trail for the School (and possibly the police) and demonstrate that visits to these sites were carried out for child protection purposes.

The E-Safety Officer will retain the completed IRT for evidence and reference purposes and will record all incidents and actions taken in the School's E-Safety Incident Log as well as any other relevant areas (e.g. Bullying or Child Protection recording procedure). After any investigations are completed, the School will debrief as appropriate, identify lessons learnt and implement any changes required.

Monitoring and Review

The E-Safety Policy will be reviewed by the Governing Body every three years and the Schedule will be formally reviewed by the E-Safety Group annually; or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.

Appendix 1 – Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's 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 and 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 without first logging out or locking my login as appropriate.
- 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 the Data Protection Act 1988. 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 E-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 E-Safety Officer 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 protect the devices in my care from unapproved access or theft.
- 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 E-Safety policy which covers the requirements for safe ICT use and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the E-Safety Officer and Designated Safeguarding Lead (DSL) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the E-Safety Officer 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 E-Safety Officer as soon as possible.

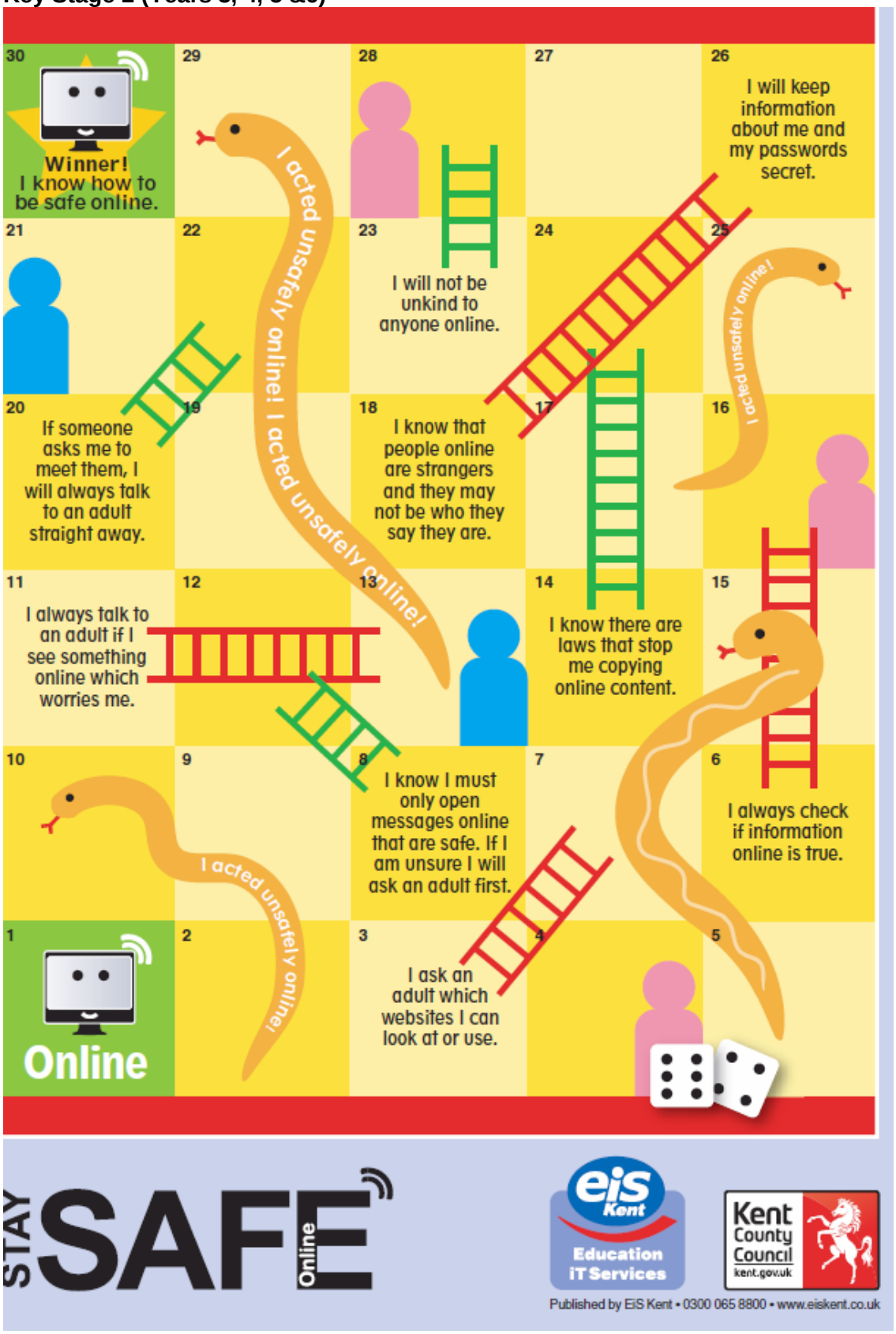
- My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via School approved communication channels e.g. via a 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 Senior Leadership team and/or Head Teacher
- 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 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 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 E-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 E-Safety Officer, or in their absence the Head Teacher.
- I understand that my use of the School's ICT system may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of ICT systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

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 as fully as possible, especially regarding attendance, behaviour, e-safety 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 refrain from publicly discussing any issues they may have with the school on social media. Not only do these get reported to the school, they can prevent parents raising concerns via the preferred method i.e direct contact.

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

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).

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.

Signed _____ Date _____

Parent of _____ Class _____

Appendix 5 - Emerging Technologies

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed when appropriate	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission – must be handed in	Not allowed
Mobile phones may be brought to School	✔						✔	
Use of mobile phones in lessons when appropriate to pupil's learning		✔						✔
Use of mobile phones in social time		✔						✔
Taking digital/videos on School owned mobile phones / cameras		✔					✔	
Taking digital/videos on personal mobile phones / cameras				✔				✔
Use of other mobile devices e.g. tablets, gaming, etc… if related to learning		✔					✔	
Use of personal email addresses in School, or on School network on own phones in social time		✔						✔
Use of School email for personal use for exceptional circumstances		✔						✔
Use of messaging apps if related to learning		✔					✔	
Use of social media if related to learning		✔					✔	
Use of blogs, wikis and other publishing sites if related to learning		✔					✔	

Appendix 6 - Unsuitable / inappropriate activities

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✔
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✔
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✔
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✔
	pornography				✔	
	promotion of any kind of discrimination				✔	
	threatening behaviour, including promotion of physical violence or mental harm				✔	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute				✔	
Using School systems to run a private business					✔	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School					✔	
Infringing copyright					✔	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✔	
Creating or propagating computer viruses or other harmful files					✔	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✔	
On-line gaming (educational)			✔			
On-line gaming (non-educational)			✔			
On-line gambling					✔	
On-line shopping / commerce – nominated users only				✔		
File sharing when relevant to learning and with permission when related to learning or School business only				✔		

Use of social media when related to learning or School business only			✔		
Use of messaging apps when related to learning or School business only			✔		
Use of video broadcasting e.g. YouTube when related to learning or School business only			✔		

Appendix 7 – E-Safety Incident Reporting (Bother Actions)