Policy: E-SAFETY POLICY **St Crispin's CP Infant School, Westgate-on-Sea**	Statutory: No Last Review: Autumn 2017 Next Review: Autumn 2018

Signed…….. Date…….……

Chairman of the Governors

Signed…….…. Date……..

Headteacher

St Crispin's C.P.I School
E-Safety Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

The Headteacher, Deputy Headteacher, Computing leader, Technician, E-safety Governor and Bursar.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review This e-safety policy was approved by the *Governing Body on 18th December 2017*

The implementation of this e-safety policy will be monitored by the senior leadership team and the e-safety governor.

The e-safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: December 2018, following a review meeting in the summer of 2017.

Should serious e-safety incidents take place, the school will follow the Kent response to incident flowchart

Scope of the Policy

This policy applies to all members of the school community (including staff, students / 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 school will respond to any incident of cyber-bullying, or any other e-safety incident by following the school behaviour policy.

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

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 Full Governing Body receiving regular information about e-safety incidents. 2 members of *the Governing Body* have taken on the role of e-safety governors (combined with their role of the safeguarding governors). The role of the e - safety governor will include:

• *regular meetings with the e-safety co-ordinator (Headteacher)*

• *regular monitoring of e-safety incident logs*

• *reporting to FGB*

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 co-ordinator.*

• The Headteacher and Computing Leader should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart (response to incident) on dealing with e-safety incidents – included in a later section.

• The Headteacher and Senior Leaders are responsible for ensuring that the e-safety co-ordinator 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 governors with responsibility for e-safety will gather pupil voice with regard to e-safety.

E-Safety Coordinator:

The role of e-safety co- ordinator will be shared between the Computing Leader (deputy DSL) and the Headteacher (DSL).

They will:

• lead the e-safety committee

• take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents

• ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• provide training and advice for staff

• liaise with the Local Authority / relevant body

• liaise with school technical staff

• receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Log sheets to be found in e-safety file in staff room).

• meet regularly with e-safety governors to discuss current issues, review incident logs and filtering issues (the school currently using a filtering service provided by EIS (a specialist ICT service provider for Kent)

• attend relevant meetings of governors

Any incidents will be dealt with by the Computing Leader in consultation with the Headteacher.

Technician:

The Technician is responsible for providing advice so that the school's technical infrastructure is secure.

• Staff users may only access the networks and devices through a properly enforced password protection policy. Pupils will have limited access to the network.

• The school will work with KCC and the School's Broadband team to ensure that systems to protect pupils are reviewed and improved.

• The use of the *network / internet / remote access / email* will be monitored in order to establish misuse or attempted misuse, If any misuse is discovered it be reported to the *Headteacher* for investigation.

All staff that have access to computers

are responsible for ensuring that:

• they have an up to date awareness of e-safety matters and of the current school / e-safety policy and practices

• they have read, understood and signed the Staff Acceptable Use Policy (AUP)

• they report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation / action / sanction

• all digital communications with parents / carers should be on a professional level and only carried out using official school systems. There should be no digital communication with pupils.

• e-safety is embedded in all aspects of the curriculum and other activities.

• pupils understand and follow the e-safety and acceptable use policies.

• pupils are developing a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• in line with the Prevent Duty, pupils will be encouraged to evaluate information that they access online at a level appropriate to their age.

• staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- when using the iPads staff will note which pupils were using which device and record in the folder on top of the iPad trolley - this will enable staff to identify which pupil had access to the machine at a given time.

• in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use. Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials that are designed for children e.g. the South West Grid for learning search engine (http://www.swiggle.org.uk/). Staff will be aware of the processes that the school has for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (DSL)

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

E-Safety Group / SLT:

The E-Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safety. Members of the *E-safety Group* (or other relevant group) will assist the *e-safety co-ordinators* with:

• the production / review / monitoring of the school e-safety policy / documents.

• consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision.

• monitoring improvement actions identified through use of e-safety monitoring tool.

Pupils:

• are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy and the school e-safety rules.

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events

Policy Statements

Education –pupils

We encourage our pupils to take a responsible approach to e-safety. 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.

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 and will be provided in the following ways:

• A planned e-safety curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited

• Key e-safety messages should be reinforced throughout the curriculum.

• When appropriate pupils will be taught in all lessons to be critically aware of the materials they access on-line and discuss the information.

• Pupils should be helped to understand the need for the e-safety rules we use in school and be encouraged to adopt safe and responsible use both within and outside school.

• Staff should act as good role models in their use of digital technologies, the internet and mobile devices

Education – parents / carers

Many parents and 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 / regulation of the children's on-line behaviours. Parents 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 therefore seek to provide information and awareness to parents and carers through:

• *Letters, newsletters, web site*

• *Parents / Carers evenings / sessions*

• *High profile events / campaigns eg Safer Internet Day*

• *Reference to the relevant web sites*

Education & Training – staff / volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as appropriate.

This E-Safety policy will be shared with all teaching staff

Training – governors

Governors should take part in e-safety training / awareness sessions provided by the school.

Technician

• All adult users will be provided with a username and secure password by the Technician (or Computing Leader) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Pupils will use group or class log-ins to access the network; in order to access the internet they will need to individually log onto the network using their 'Purple Mash' logins. Each child will have his/her own unique login for 'Purple Mash' which will be kept safely by the class teacher.

• The "master / administrator" passwords for the school system, used by the Technician must also be available to the Headteacher and/or Computing Leader and kept in a secure place.

• Identified staff are 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 (Bursar – admin software / Computing Leader - curriculum software).

• The school has provided enhanced user-level filtering (allowing different filtering levels for different groups of users – staff / pupils etc)

• Any "guests" (e.g. trainee teachers, agency supply teachers, visitors) will use a guest login and will have limited access to the school systems and internet i.e. no access to youtube. A list will be kept in the office of which login has been given to which visitor in order that we can monitor usage.

• Staff will use any school device in line with the staff acceptable use policy that states that any hardware and software provided by the workplace for staff use can only be used by members of staff and only for educational use, both inside and outside of school.

• Staff will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Computing Leader.

• Staff will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. Sensitive data will be removed from the school site on a password protected laptop or an encrypted memory stick. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

Use of digital and video images

See separate policy.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Kept no longer than is necessary

• Processed in accordance with the data subject's rights

• Secure

• Only transferred to others with adequate protection.

For further details please see our Data Protection policy.

Communications

When using communication technologies the school considers the following as good practice:

• The official school / email service may be regarded as safe and secure and maybe monitored.

• Users must immediately report, to the Headteacher (or Deputy Headteacher), 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.

• Any digital communication between staff and parents / carers will be professional in tone and content and use the school email account.

• Whole class email addresses may be used for educational use.

• Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

• Personal information should not be posted on the school website and only official email addresses should be used.

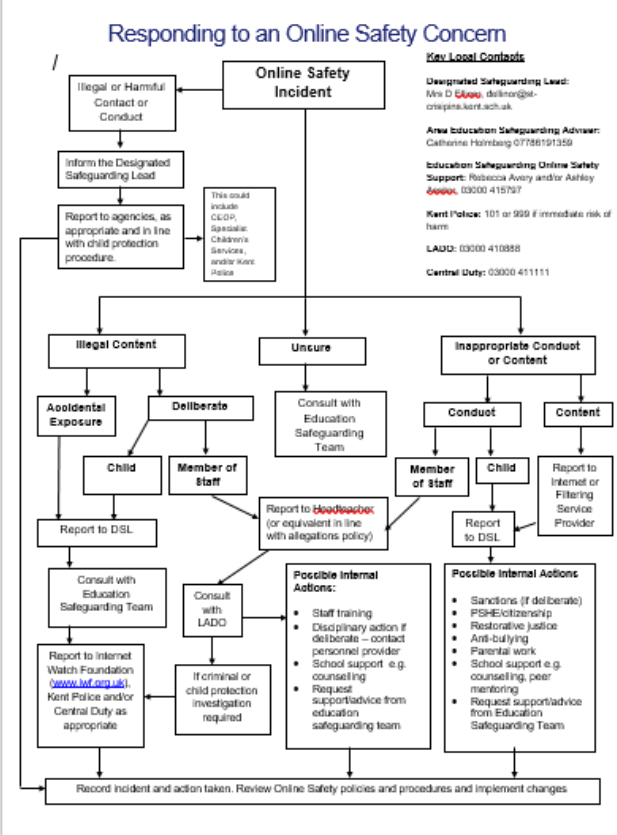
Social Media

School staff should ensure that:

- No reference is 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 are not 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 by individual members of staff.
- They do not state where they work in their social media profile.

Illegal Incidents

If there is any suspicion that any web site(s) accessed may contain child abuse images, or if there is any other suspected illegal activity, staff will follow the 'response to incident' flow chart displayed in each classroom and below.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and

content visited are closely monitored and recorded (to provide further protection.

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

• Internal response or discipline procedures

• Involvement by Local Authority or national / local organisation (as relevant).

• Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

• incidents of 'grooming' behaviour

• the sending of obscene materials to a child

• adult material which potentially breaches the Obscene Publications Act

• criminally racist material

• other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps 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 completed form should be retained by the group for evidence and reference purposes.

Acknowledgements

This policy has been created using a template produced by SWGfL.