CROMPTON HOUSE CHURCH OF ENGLAND SCHOOL

Loving God - Caring for Each Other – Achieving Excellence

E-SAFETY POLICY AND GUIDANCE
(to be read in conjunction with the IT acceptable Use and GDPR Policy)

Scope

This policy applies to all members of the *Crompton House School* community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of academy 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 students 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.

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.

1. Purpose

The focus of this policy is to ensure that existing policies (such as those on child protection, bullying, the curriculum, and behaviour) are applied to the digital environment.

1.1. These guidelines set out the rules and parameters relating to e-safety so that all members of staff, students and the school community are aware of what constitutes appropriate and inappropriate use.

1.2. Failure to comply with the provisions of this policy and the accompanying guidelines may lead to disciplinary action being taken against a member of staff or student and may in some instances be deemed gross misconduct or grounds for exclusion.

1.3. The policy will be reviewed after a 12-month period of operation and if necessary, more frequently.

1.4 These guidelines apply to all staff that have access to any ICT (Information Communication Technology) services provided by Crompton House School. The policy covers use of ICT both on and off School premises and at any time and in any place.

1.5 Policies and guidelines will be available online via the School's website and on Sharepoint.

1.6 Any major revisions to these policies or guidelines will be notified through an appropriate medium.

1.7 New employees will not be given access to e-mail, the internet or any of Crompton House IT systems until they have seen and accepted these policies. This will be the responsibility of the Senior Manager with responsibility for new staff induction.

1.8 In the event that an employee ceases to be employed by Crompton House School, their school system account(s), e-mail account(s) and any other accounts will be suspended, and any stored data removed at the school's discretion.

Responsibilities

This e-safety policy has been developed by the Crompton House e-safety working group made up of:

- Headteacher- K. Newell
- Designated Safeguarding Lead – Danyel Dunkley
- Staff- IT working group
- Governors

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 *Governors admissions and student support Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor*. The role of the E-Safety *Governor* will include:

- *regular meetings with the Safeguarding officer*
- *regular monitoring of e-safety incidents held within the safeguarding logs*
- *regular monitoring of filtering and discussion around matter arising*
- *reporting to relevant Governors*
- *Jonathan Swift is the nominated Link Governor.*

Headteacher

- **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**.
- **The Headteacher and another member of the Senior Leadership Team 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.**
- *The Headteacher and delegated Senior Leaders are responsible for ensuring staff receive suitable training to enable them to carry out their e-safety roles.*

Monitoring & Filtering:

- In line with KCSIE 2020 (subsequent incarnations of KCSIE 21 & 22 & 23), the school has a mechanism with which to apply appropriate filters and monitoring systems. In school this is monitored by Impero software.

ICT team leader / Technical staff:

- The ICT team leader is responsible for ensuring:
- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the use of the *network / internet / office 365 / TEAMS/ remote access /* email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher.

Teaching and Support Staff

Teaching and Support staff 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
- they report any suspected misuse or problem to a member of the leadership team for investigation.
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they 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
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- *When setting remote learning opportunities and using TEAMs as a learning platform, staff are mindful of their statutory duties to safeguard young people and set work and conduct themselves in a professional manner equivalent to standard professional conduct within a classroom environment*
- *See' Remote Learning Policy 2022: Professional Conduct and E Safety*

Designated Safeguarding Lead

- 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 / strangers

- potential or actual incidents of grooming
- cyber-bullying
- all issues that may link to safeguarding concerns

Students

- are responsible for using the *school* digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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.

2. Policy statements

Parents

Parents 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
- access to parents' sections of the website / on-line student / pupil records
- their children's personal devices in the school / academy (where this is allowed)

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* 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 should be provided as part of IT lessons and should be regularly revisited. At school we teach students to understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct, and know how to report concerns**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities**
- **Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Students should be helped to understand the need for the student Acceptable Use Agreement and 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*
- *in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

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:

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g.* www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Training – Governors

Governors should take part in e-safety training sessions, when this has a particular importance for those who are members of any sub-committee involved in technology/e-safety/health and safety/ safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association/ or other relevant organisation.
- Participation in school training/ information sessions for staff or parents (this may include attendance at assemblies).

2.1. The policies and these guidelines have been approved and adopted by the Leadership Group and Governing Body.

2.2. It is the responsibility of the Leadership Team that the policies and guidelines are properly implemented and policed.

2.3. All staff, with access to e-mail on personal or work equipment, the internet and school IT systems (including laptops on or off site, PDAs, mobile phones, memory sticks, tablets and all other electronic equipment) will be held responsible for complying fully with the school's e-safety usage policy and guidelines.

2.4. The School will make every effort to ensure that all School owned equipment (including staff laptops) are running up to date anti-virus software, is updated regularly and that access to the internet is monitored and filtered. All data held on school equipment will be kept as secure as possible and never shared with third parties without the express permission of the owner.

3. Use of Email

3.1. Digital communications with pupils (e-mail, online chat, office 365 / TEAMS, voice etc.) should be on a professional level and only carried out using official school systems.

3.2. Students and staff communication via email should be done so using the school email system only.

3.3. Under no circumstances should staff contact pupils/carers or conduct any school business using their personal e-mail address.

3.4. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) but not for contact with parents/pupils.

Mobile Phones

3.5. School mobile phones only should be used to contact parents/carers/students when on school business with students off site.

3.6. Staff should not be using mobile phones in school during working hours when in contact with children unless in cases of emergency.

3.7. Students should adhere to the rules and guidelines set out in the Behaviour Policy/Bring your own Technology Agreement regarding mobile phone use and other technology in school.

Removable Data Storage Devices

3.8. External drives including memory sticks must not be used to store or transfer confidential material and any pupil data.

3.9. Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptops, for e.g. photos, videos, bank statements.

3.10. Students should have separate storage devices for personal and schoolwork.

Data storage

3.11. Personal or sensitive data should not be stored on cloud-based sites outside of Office 365, such as dropbox.

3.12. Cloud based storage which is shared with students must only be set up using a school email and password.

3.13. All should ensure any screens are locked before moving away from a computer during the normal working day to protect any personal, sensitive, confidential, or classified data.

4. Personal use of the Internet

4.1. Staff may access the internet for personal use in their own time on the understanding that they comply with the provisions within this policy. Users should be aware that all internet activity is recorded. The school reserves the right to monitor usage in accordance with the human Rights Act 1998 and the Regulation of Investigatory Powers Act 2016.

4.2. Staff should not download any material that is not directly related to their job responsibility. This especially relates to screensavers, images, games, etc.

4.3. Staff must not use the internet at any time for either private commercial purposes or personal gain.

4.4. Employees may make personal purchases on the internet in their own time and at their own risk.

4.5. Use of games is prohibited. Games must not be downloaded from the internet or installed onto machines.

Misuse and Inappropriate Websites

4.6 The school filters unsuitable websites.

4.7 Staff must not knowingly use the School's internet facilities and hardware at any time to access or download the following types of information:

- Criminal information, e.g. racist or terrorist propaganda;
- Pornography, abusive, defamatory, offensive, obscene, or malicious information;
- Information that makes improper or discriminatory reference to person's race, colour, religion, sex, age, creed, national origin, disability, or physique;

  Any information that may be perceived as damaging or likely to damage the School's reputation.

4.8 If you find yourself connected to an inappropriate site inadvertently, you should disconnect from that site immediately and notify your line manager. The line manager concerned should then contact the IT Support Team who will ensure the site is blocked.

4.9 Because individuals may consider a wide variety of material offensive, users should not store, view, print or redistribute any material that is not directly related to the user's role or the School's activities.

4.10 There are systems in place to monitor and record all internet usage. No user should have any expectation of privacy as to his or her internet usage. Analysis of this information may be issued to Managers if thought appropriate and any inappropriate use will be reported.

Social Media

4.11 Staff members must not have contact through any personal social medium with any pupil, whether from Crompton House or any other school, unless the pupils are family members. It is essential that the use of social media accounts such as Twitter are checked with the SLT.

4.12 Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

4.13 Communication between staff and pupils must be carried out using school systems only. I.T. can give advice on the most appropriate medium for your communication.

4.14 Staff members and governors **must** decline 'friend/follow requests' from pupils they receive in their personal social media accounts. Any requests should be referred to the Safeguarding Lead.

4.15 On leaving Crompton House School, staff members must not contact Crompton House School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

4.16 School e-mail addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

4.17 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships.

4.18 Staff members must set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. Staff should consider their professional status and the reputation of the School before posting content on their personal sites.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 policies to reduce the likelihood of the potential for harm:

4.19 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

4.20 In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.

*4.*21 Staff and volunteers are allowed to take digital / video images to support educational aims provided the school holds permission to do so. Staff must follow school policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on school equipment where possible. If images are taken on the personal equipment of staff these should be uploaded to school systems and then deleted off the personal equipment.

4.22 Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

4.23 Students must not take, use, share, publish or distribute images of others without their permission.

4.24 Photographs published on the website, or elsewhere that include students/staff will be selected carefully and will comply with good practice guidance on the use of such images.

4.25 Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

4.26 Parents/carers will inform the school if they do not wish their son/daughter to be photographed.

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.

This document should be read in conjunction with the IT Acceptable Use and GDPR Policy.

Document CSC-ESP2022/October 2023 adopted by Curriculum Committee

Date: 17th October 2023

Signed (Chair)……J Swift……..

Print Name ……Jonathan swift……..

Date of next review: October 2024

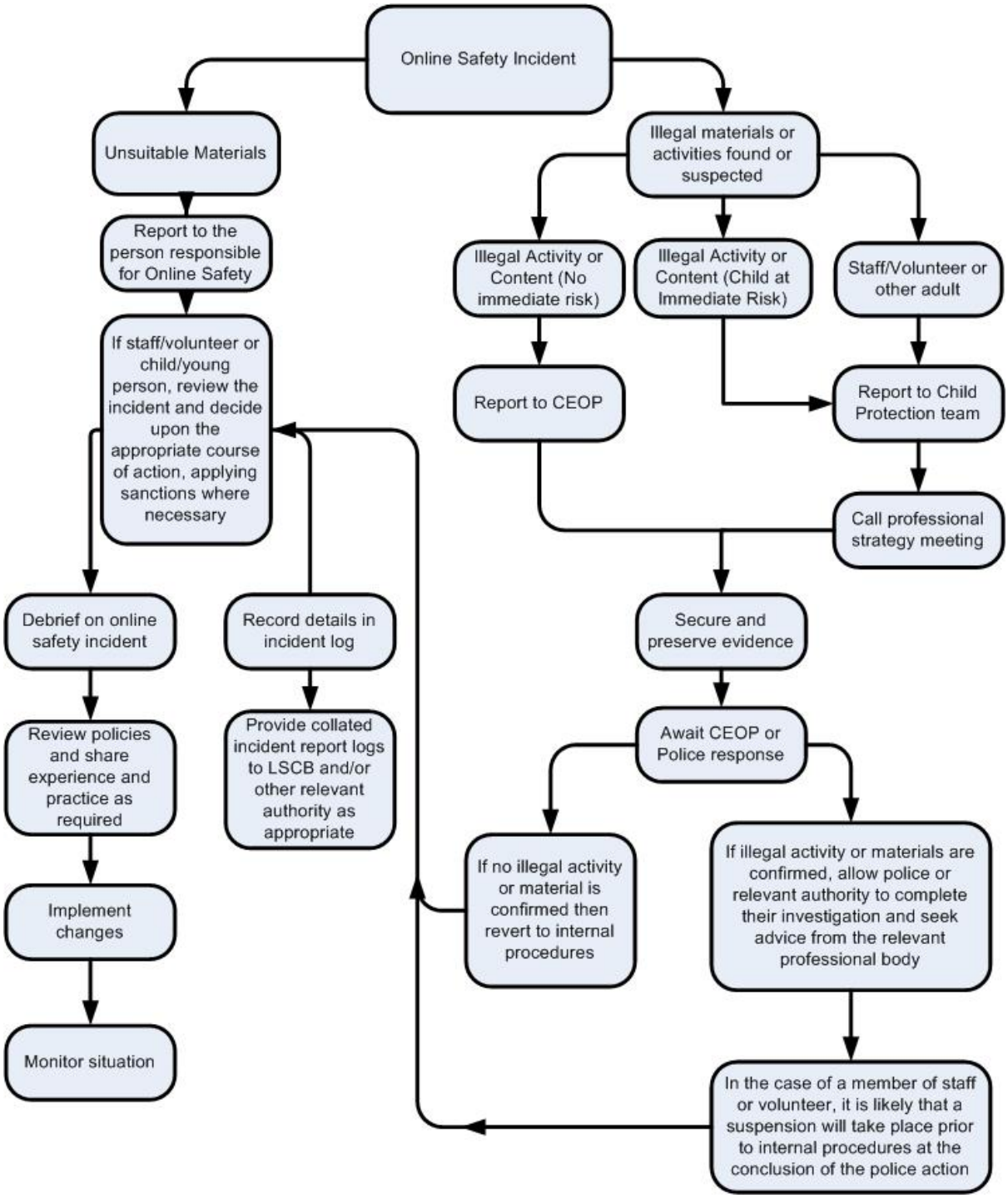
	Staff & other adults				Students / Pupils Years 7 -11			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones / cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								

X[1] See Mobile Phone Policy
X*At the end of the school day (after the final bell)

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*18th October 2022*
The implementation of this e-safety policy will be monitored by the:	*Governors admissions and student support Sub Committee*
Monitoring will take place at regular intervals:	*Once a year in September*
The *Governing Body / Personnel or Pupil support Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Once a year*
The E-Safety Policy will be reviewed 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. The next anticipated review date will be:	*October 2023*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police*

Responding to incidents of misuse – flow chart



Training Needs Audit

Training Needs Audit Log

Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date