Christ Church

Church of England Primary School

Being Thankful, Celebration, Fairness, Forgiveness, Honesty, Love for All

E-SAFETY POLICY

The ethos of our school is embedded in our key Christian values

Honesty

Forgiveness

Love for all

Celebration

Fairness

Being Thankful

Ambition

Resilience

This school is committed to safeguarding and promoting the welfare of children and this policy supports this commitment.

Policy approved: June 2018 *Review Date: June 2019*

Embedding Pupil Safeguarding Awareness in the Curriculum

All teachers incorporate elements of safeguarding into their lessons where appropriate. This involves:

- Informal conversations;
- Teacher/pupil discussions;
- Briefings for outings and trips (road safety/stranger danger etc) ;
- The implementing of our e-Safety Policy regarding ICT usage;
- An awareness of any potential hazards in lessons – identifying risks and dangers;

Safeguarding is also about pupils' emotional well-being. Teachers encourage pupils to speak out if there is something worrying them, or if they are aware of, or witness something unacceptable, untoward or disturbing. Teachers promote tolerance and respect for each other and acceptance of individual differences. Teachers help pupils develop confidence and resilience and discuss what to do if things go wrong. They are approachable and show their willingness to help pupils at all times.

British Values

At Christ Church C of E Primary School we promote the fundamental British values of democracy, the rule of law, individual liberty, and mutual respect and tolerance of those with different faiths and beliefs.

This includes:

- paired and group work as sharing and working together
- making choices with an understanding that the freedom to choose and have other views is respected and tolerated
- debating social issues with an understanding of how people can influence decision-making through the democratic process
- an appreciation that school rules protect individual children and is essential for their wellbeing and safety
- an acceptance that other people having different faiths or beliefs to oneself (or having none) are accepted and tolerated without discrimination through school council elections, persuasive writing, and by promoting our Christian school values and Fruits of the spirit as guidelines for behaviour choices.

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible and self-aware approach. The education of pupils in e-safety is an essential part of the school's e-safety provision.
E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Children and young people need the support and help of the school to recognise and avoid e-safety risks and build their resilience/awareness of actions to take when such situations arise. Through embedding e-safety throughout the primary curriculum, children will learn to appreciate what it is to be a valued 'netizen' online.

The Law

Our E-Safety Policy has been written by the school, using advice from government guidance. The Policy is part of the School's Development Plan. As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Roles and Responsibilities

The Headteacher:

- has a duty of care for ensuring the safety (including e-safety) of members of the school community
- liaises with school technical staff
- Ensure the policy is implemented, communicated and compliance with the policy is monitored.
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training.
- and the Senior Leadership Team (SLT) are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, using the Kingston LSCB Incident Procedure flowchart and that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place, as outlined by the Kingston LSCB Incident Procedures flowchart.
- *Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites.
- Ensure that all reported incidents of cyber bullying are investigated.
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material.

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely.
- Monitor and supervise pupils' internet usage and use of other IT resources.
- Adhere to the Acceptable Use Agreement.
- Promote e-safety and teach e-safety units as part of computing curriculum.

- Engage in e-safety training.
- Only download attachments/material onto the school system if they are from a trusted source.
- When capturing images, videos or sound clips of children, only use school cameras/iPads or recording devices. It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the Local Authority are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively.
- Adhere to the acceptable use agreement when in school.
- Have due regard for the importance of e-safety in school.

The following section outlines the roles and responsibilities of individuals working within / associated with the school community:

Child Protection / Safeguarding Designated Person will aid staff in empowering children through their understanding of staying safe online and what actions to take if not. They will 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

Technical staff:

On-site technical staff will ensure:

- 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 / other relevant body E-Safety Policy / Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering protocol is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator.

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 through attendance of e-safety staff training sessions
- they have read, understood and signed the Staff Code of Conduct for ICT Agreement
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with students / pupils / 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
- children understand and follow the e-safety and acceptable use policies as built into the Home School Agreement
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies 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, children 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

Children are responsible**:**

- for using the school digital technology systems in accordance with the Rules for Responsible Internet Use (Home School Agreement)
- 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 understand potential risks involved with the taking / use of digital images and how they may be linked to cyber-bullying.
- will 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 responsibility

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. 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
- their children's personal devices in the school (where this is allowed)

Education

Teaching and Learning

The school will actively teach E-safety at an age-appropriate level. The school in part follows a scheme of work for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics. E-safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Pupils

E-safety is 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 is provided in most lessons and will be made implicit in planning when there is use of the internet or digital technologies. Planning is directed at how to stay safe online and outlines current e-safety issues, ensuring children are aware of current risks.
- Key e-safety messages will be reinforced as part of a planned programme of activities
- Children are made aware of the accuracy of online information and are educated on how to determine whether websites are factually true.
- Children are taught to respect copyright when using material accessed on the internet so as to avoid plagiarism.
- Children are helped to understand why the school have rules for accessing the internet and they will be encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their understanding of current technology. They should inform their own understanding of current e-safety issues by being aware of new and existing online practices amongst children.
- In lessons where internet use is pre-planned, it is best practice that children are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (with the Headteacher's authorisation) can temporarily remove those sites from the filtered list. Any request to do so, should be auditable via LGFL Webscreen, with clear reasons for the need.

Parents / carers

Parents and carers may only have 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 some of the following:

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers consultations
- High profile events e.g. Safer Internet Day

- E-safety evening
- Reference to relevant web sites / publications

Where children inform Teachers / Staff that they are accessing age inappropriate material outside of school, teachers should, under their duty of care, inform parents of the disclosure and make them aware of advice in regards to managing e-safety risks at home.

Staff / Volunteers

Staff will receive e-safety training annually and understand their responsibilities, as outlined further in this policy. Training will be offered as follows:

- A programme of formal e-safety training will be made available to staff. This will be updated and reinforced annually. 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 will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Staff Code of Conduct for ICT Agreement
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) 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 / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Governors

Governors will take part in e-safety training sessions, with particular importance for those who are members of any group involved in technology / e-safety / health and safety / child protection. This will be offered via:

- Participation in school training / information sessions for staff and/or parents

Technical

Monitoring safe and secure systems

Internet access is regulated by Strictly supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff take responsibility for safeguarding confidential data saved to laptops, ie use of strong passwords. If personal data has to be saved to other media, eg data sticks, it is to be encrypted or strong password protected. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This will include:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices.
- The Technical Support 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
- Appropriate security measures are in place to protect and secure all equipment and infrastructure from accidental or malicious attempts which might threaten the security of the school systems and data. These should be updated regularly.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (e.g. use of encrypted USB sticks.)

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to Strictly
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email

The school website

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking, Social Media and Personal Publishing (blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g. Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home. School and class blogs are run through the school website and are password protected.

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- 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
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

Use of digital and video images

Staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Children will be informed of the risks attached to publishing their own images on the internet e.g. on social networking sites through the e-safety curriculum.
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images must not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in the digital / video images.
- Children must not take, use, share, publish or distribute images of others without their permission
- Written permission from parents or carers will be obtained before photographs of children are published on the school website as outlined in the Home School Agreement
- Children's' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.

Personal mobile phones and mobile devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.

Emerging Technologies

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Children will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Home School Policy.

The following table shows how the school currently considers the benefit of using emerging communications technologies for education in comparison to the risks:

	Staff				**Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Not allowed	Allowed	Allowed at certain times	f permission and authorised by the Headteacher.
Mobile phones may be brought to school	✓						✓*	
Use of personal mobile phones in lessons				✓	✓			
Use of personal mobile phones in social time	✓				✓			
Taking photos on mobile phones (school owned)				✓				✓**
Use of other mobile devices (e.g. tablets, gaming devices, cameras)	✓							✓
Use of personal email addresses in school, or on school network			✓**		✓			
Use of school email for personal emails				✓	✓			

Use of messaging apps (e.g. Skype, MSN)				✓	✓			
Use of social media (e.g. Twitter)			✓		✓			
Use of blogs (the school blog site)			✓***					✓

* Before and after school – Not to be kept during the school day.

** As directed by SLT in cases of emergency or for new staff.

*** To be managed by directed staff.

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and children will therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access.)
- Users must immediately report, to the nominated person – in accordance with the school policy, 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 children or parents / carers (email) must be professional in tone and content. These communications must only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- KS2 may be provided with individual school email addresses for educational use.
- Children will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Where required by the Local Authority any data relating to children should be sent using the USO FX2 and not by email.

Social Media - Protecting Professional Identity

With the rise of Social Media websites, it is important that all members of the school community remain professional and secure online.
School staff must ensure that:

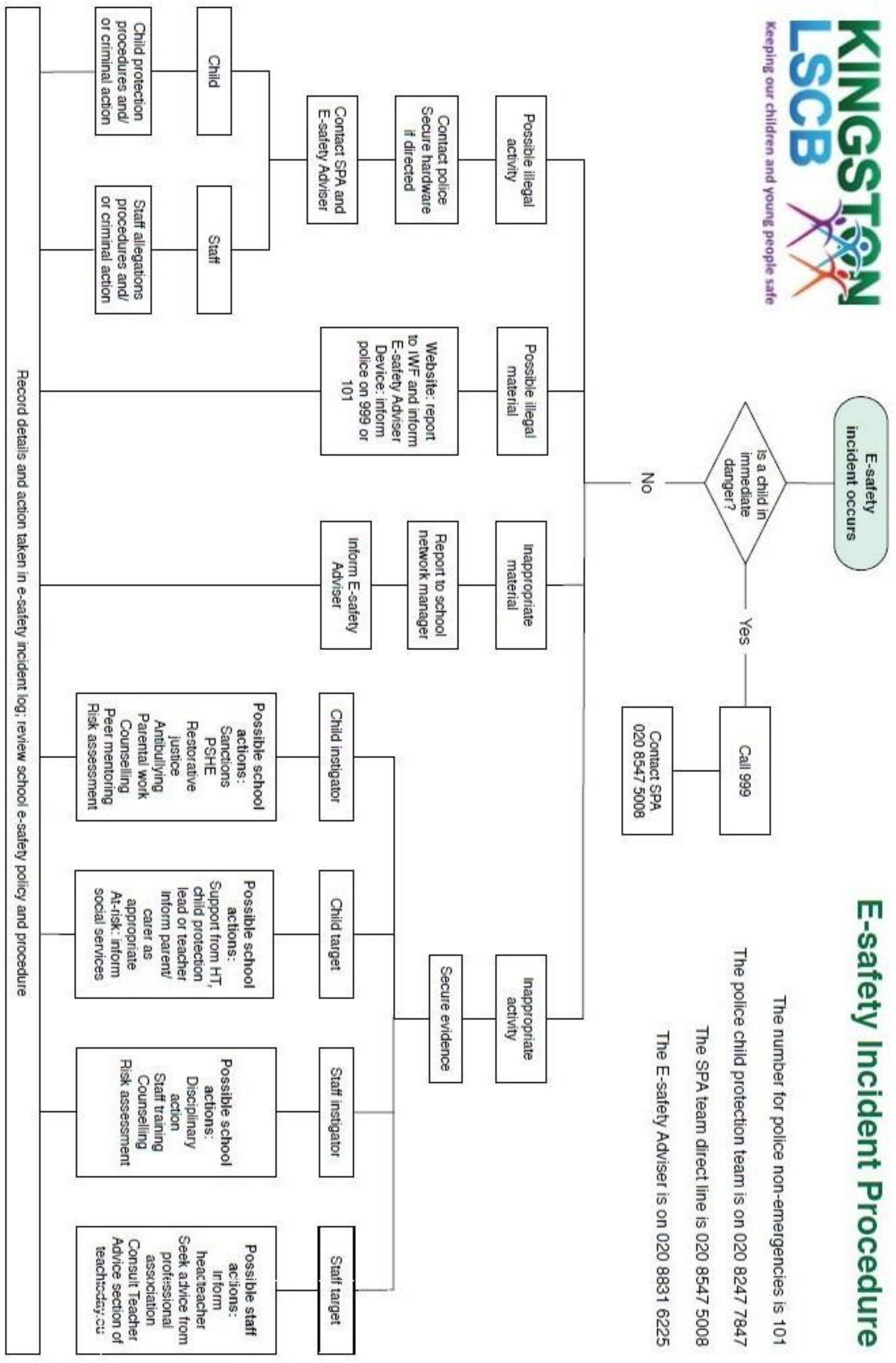
- No reference should be made in social media to children, parents / carers or school staff, especially in cases where the individual or school would be put into disrepute.
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They are aware of the Social Networking Policy

The school's use of social media for professional purposes will be checked regularly by directed staff to ensure compliance with the Social Networking Policy, Data Protection Act and Digital Image and Video Policies.

Responding to incidents of misuse

The following flowchart, as released by Kingston LSCB, outlines current procedures that should be taken when an e-safety incident arises. This should be used to inform members of the school community on actions to take in varying circumstances.

July 2018


KINGSTON LSCB
Keeping our children and young people safe
E-safety Incident Procedure
The number for police non-emergencies is 101
The police child protection team is on 020 8247 7847
The SPA team direct line is 020 8547 5008
The E-safety Adviser is on 020 8831 6225
E-safety incident occurs
Is a child in immediate danger?
Yes
Call 999
Contact SPA 020 8547 5008
No
Possible illegal activity
Contact police Secure hardware if directed
Contact SPA and E-safety Adviser
Child
Staff
Child protection procedures and/ or criminal action
Staff allegations procedures and/ or criminal action
Possible illegal material
Website: report to IWF and inform E-safety Adviser Device: inform police on 999 or 101
Inappropriate material
Report to school network manager
Inform E-safety Adviser
Inappropriate activity
Secure evidence
Child instigator
Possible school actions: Sanctions PSHE Restorative justice Antibullying Parental work Counselling Peer mentoring Risk assessment
Child target
Possible school actions: Support from HT, child protection lead or teacher Inform parent/ carer as appropriate At-risk: inform social services
Staff instigator
Possible school actions: Disciplinary action Staff training Counselling Risk assessment
Staff target
Possible staff actions: inform headteacher Seek advice from professional association Consult Teacher Advice section of teachtoday.eu
Record details and action taken in e-safety incident log; review school e-safety policy and procedure

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. It is intended that incidents of misuse will be dealt with through normal behaviour procedures.

Contacts and References

CEOP: (Child Exploitation and Online Protection Centre): **http://www.ceop.police.uk**
Childline: **http://www.childline.org.uk**
Childnet: **http://www.childnet.com**
Click Clever Click Safe Campaign: **http://www.nidirect.gov.uk/click-clever-click-safe**
Cybermentors: **http://www.cybermentors.org.uk**
Digizen: **http://www.digizen.org.uk**
Internet Watch Foundation (IWF): **http://www.iwf.org.uk**