KING EDWARD'S WHOLE SCHOOL POLICY DOCUMENT

Title: E-safety Policy

Policy Category	Academic/Pastoral
Status	Under review
Approved by	Governing Board
Current Author	WJQ
Last Approved/Updated	Oct 2023
Frequency of Review	Annual
Date of Next Review	Spring Term 2025
Application	Whole School
Responsibility	WSMT

Contents

A. INTRODUCTION

1. This policy applies to King Edward's Pre-Prep, Junior and Senior Schools. This policy is reviewed annually by the Governing Body, or more regularly in the light of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. *This policy is based upon the model policies issued by ISBA and The Key and adapted for King Edward's School*.

2. The implementation of this policy will be monitored by the Designated Safeguarding Lead (***DSL***)and the WSMT. Monitoring by the Governing Body will take place annually. The Governing Board will receive a report on the implementation of this policy generated by the DSLs (which will include anonymous details of online safety incidents) at regular intervals.

3. All online safety incidents should be reported to the School's DSL (see Section E below)**:**

4. All serious online safety incidents should be reported to the appropriate external person/agencies including, for staff, the Community Safety and Safeguarding Partnership Designated Officer, local police (see section E).

5. The School will monitor the impact of the policy:
    - using logs of reported incidents on My Concern (pastoral staff)
    - by investigating reports of suspicious activity and providing evidence from logs; (IT staff)
    - by recording and reporting on internal internet activity (IT staff)

6. e-Safety can also be called 'internet safety', 'online safety' or 'web safety'. e-Safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (eg text messages, gaming devices, email etc).

B. SCOPE OF THE POLICY

1. This policy applies to all members of the School community (including staff, pupils, volunteers, governors, parents, visitors and community users) who have access to and are users of the School IT systems, both in and out of the School.

2. The School will deal with online safety incidents in accordance with the procedure set out in this policy and associated school policies and government guidance. See list at end of policy. Where known, the School will inform parents of incidents of inappropriate online behaviour that take place out of school.

3. It is essential that children are safeguarded from potentially harmful and inappropriate online material. The use of technology has become a significant component of many safeguarding issues including Child Exploitation (CE), radicalisation and sexual predation. Young people can be both victims and perpetrators of online abuse.
   Online safety is reflected in all relevant policies and is considered when planning the curriculum, any teacher training, the role and responsibilities of the DSL and any parental engagement.

4. The four main areas of risk in the use of technology are:

   Content: being exposed to illegal, inappropriate or harmful material; e.g. pornography, fake news, racist, misogynistic, self-harm, suicide, anti-semitic, radical and extremist;

Contact: being subject to harmful online interaction with other users; e.g. child-on-child abuse and peer pressure, sexual violence and sexual harassment; and adults posing as children or young adults for the purposes of grooming children. Abuse that occurs online or outside of the school should never be downplayed and should be treated equally seriously as any other safeguarding issue;

Conduct: personal online behaviour that increases the likelihood of, or causes harm; e.g. making, sending and receiving explicit images, sharing others explicit images including nudes and semi-nudes, and online bullying;

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If there is a concern that pupils or staff are at risk, it should be reported to the DSL.

5. Remote Learning and School Closure

In circumstances where teaching and learning is provided to pupils off-site (due to school closure, for instance), teachers and non-teaching staff will communicate with pupils through the relevant approved channels; school email accounts, Teams, and the virtual learning platform.

Staff, pupils and parents are reminded that the usual arrangements for safeguarding are not affected by school closure, although procedures and policies would be reviewed and shared.

6. Reviewing Online Safety

Technology, and the risks and harms related to it evolve and change rapidly. The School regularly reviews our approach to online safety, supported by an annual risk assessment that considers and reflects the risks our children face.

C. ROLES AND RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individuals and groups within the School:

C1 Governors

Governors are responsible for the approval of, and reviewing the effectiveness of, this policy. This will be carried out by the governors' Education Committee receiving regular information about online safety incidents and monitoring reports.

Mr Kambiz Moradifar the School's **Designated Safeguarding Lead Governor (DSLG)**, is also responsible foronline safety.

The role of the Safeguarding Governor includes:

- regular meetings with the DSLs;
- regular review of anonymous details of online safety incident logs;
- regular review of e-safety curriculum inclusions and staff training
- regular review of filtering / change control logs and provision in-line with the DfE Filtering and Monitoring Standards
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- reporting to Governing Board

C2 Head and the Whole School Management Team (WSMT)
The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day-to-day responsibility for online safety will be delegated to the DSL.

The Headmaster and WSMT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

WSMT will receive regular monitoring reports from the relevant DSL.

C3 DSL
The School Safeguarding Team are listed in the School's Safeguarding policy.

They are responsible for:

1. dealing with online safety incidents in accordance with the School's Safeguarding Policy, including potential serious safeguarding issues arising from:
    - sharing of personal data;
    - access to illegal / inappropriate materials;
    - inappropriate online contact with adults / strangers;
    - potential or actual incidents of grooming;
    - cyber-bullying (see the School's Anti-bullying Policies)
    - child-on-child online abuse, including the sharing of nude and semi-nude images

2. taking day-to-day responsibility for online safety issues and having a leading role in establishing and reviewing the School's online safety policies;
3. ensuring that staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
4. arranging for training and advice on online safety to be provided for staff, governors, parents and pupils in liaison with the Deputy Head (Digital Strategy) and the relevant Head of PSHE;
5. liaising with School IT staff / the Local Authority where necessary;
6. receiving reports of all online safety incidents and recording all investigations on MyConcern
7. maintaining and regularly reviewing the online safety incidents which are logged, in order to identify potential patterns of behaviour, to determine if any changes to this policy are required and to inform future online safety developments;
8. meeting regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering;
9. reporting all serious Online Safety incidents to the WSMT

C4 IT Manager
The IT Manager is responsible for ensuring that:

- the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices which is in accordance with the School's Acceptable Use policy.
- filtering is applied and updated on a regular basis
- investigations into any online safety incident in accordance with this policy are reported to the DSL (see Section E below)
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;

- the use of the School's network and devices is logged, and records can be provided and searched on request to ensure compliance with all the Acceptable Use Policies in order that any misuse / attempted misuse can be reported to the DSL for investigation;
- the School's antivirus system definitions and web filter categories are updated automatically.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Meet regularly with the Deputy Head (Digital Strategy) to discuss security upgrades and their impact on this policy and its implementation

C5 Deputy Head (Digital Strategy)
It is the responsibility of the Deputy Head (Digital Strategy) to:
- ensure staff are aware of the safety features in place.
- communicate any changes/upgrades to online systems, which impact this policy (in conjunction with the IT Manager)
- organise training on these features, when necessary
- advise the relevant Head of PSHE in the creation of appropriate e-safety learning content for pupils to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- keep parents informed of the safety features in place and any changes
- attend any Pastoral Committee (Senior School) meetings, or other meetings in the Pre-Prep and Junior School, where e-safety is discussed

C6 Teaching and Support staff
Teaching and support staff are responsible for ensuring that:
- they have an up-to-date awareness of online safety matters and the details of this policy;
- they have read and understood the Acceptable Use Policy.
- they report any suspected misuse or problem to the DSL for investigation (see Section E 'Responding to Online Safety Incidents);
- all digital communications with pupils, parents and other members of staff should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- pupils are helped to understand and follow this policy and the AUP
- 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, pupils are guided to sites checked as suitable for their use, and any filtering issues such as any unsuitable material that is found in internet searches should be reported immediately to the IT Manager or the DSL.
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

C7 Pupils
Pupils at the School:
- are responsible for using the School digital technology systems in accordance with the AUP
- 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 personal mobile devices
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that this policy covers their actions out of school, if related to their membership of the School.

C8 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' induction evenings, parent talks, newsletters, letters, the VLE, and information about national/local online safety campaigns/literature. The School also refers parents to Parentzone, the digital parenting charity for 1-1 advice.

Parents will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events

C9 Visitors

The majority of visitors should not need to access the School's IT systems while on site. In cases where this is deemed necessary, a request will be made to the IT Support Team and a guest account, with limited access, will be made available. The visitor will have to read and accept the AUP before being allowed on the system. As soon as the access is no longer required, the account will be disabled.

D. POLICY STATEMENTS

D1 Education – Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage, and personal circumstances. However, there are some pupils, such as looked after children, or those with special educational needs and/or learning differences, who may be more susceptible to online harm or have less support from family and friends in staying safe online. The School's online safety curriculum ensures these pupils receive the information and support they need.

The online safety curriculum is broad, relevant and provides progression through EYFS and Key Stage 1 to Key Stage 4,

E-Safety within the Curriculum for Early Years Foundation Stage and Key Stage 1

At this level, use of the Internet will be heavily supervised and based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. Links will be made through the teaching of PHSE (JIGSAW) and Being Safe.

Opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided which is informed by the DfE guidance on Teaching Online safety in school (January 2023) and key online safety messages are reinforced as part of ICT lessons /PSHE /assembly programme and is regularly revisited;
- Pupils are taught in all lessons to be critically aware of the content they access online and guided to validate the accuracy of information;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are helped to understand the need for the Acceptable Use Policy 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 pupils are guided to sites checked as suitable for their use and any unsuitable material that is found in internet searches should be reported immediately to the DSL /IT Manager (see Section E below);
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the pupils visit;
- It is accepted that from time-to-time, for good educational reasons, pupils 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 make a request to unblock the site via the IT helpdesk (helpdesk@kesbath.com) in order that those sites can be removed temporarily from the filtered list for the period of study with the authorisation of the DSL. **Any request to do so, must be auditable, with clear reasons for the need**.

An outline of curriculum objectives at each level Is included in Appendix B

D2 Education – Parents

The School seeks to provide information and awareness to parents through:

- Curriculum activities
- Letters, newsletters, web site, VLE, School Gateway, the Parent Portal
- Parents induction evenings

D3 Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. The following training is provided by the DSL or Deputy Head (Digital Strategy);

- A planned programme of formal online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand this policy and the AUP for Staff.
- The DSL (or other nominated person) 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 in staff / team meetings and INSET days.
- The DSL (or other nominated person) will provide advice / guidance / training to individuals as required.

D4 Technical–Infrastructure / Equipment, Filtering and Monitoring

Monitoring and filtering of the school network and use of ICT facilities

School technical systems are managed in ways that ensure that the School meets recommended technical requirements. These systems are described in detail in the Schools' Technical Security Policy (under review) in line with the DfE Digital and technology standards in schools 2023 and Data Protection regulations.

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

D6 Data Protection

The School has a Data Protection Policy and Privacy Notices, which include statements about how personal data will be collected, processed and stored.

Staff must ensure that:

- They comply with the requirements set out in the Data Protection Policy for Staff and the AUP for Staff.
- A Privacy Impact Assessment is carried out before any new project involving personal data is implemented, to assess the impact of the project on the security of data. Speak to the Data Protection Lead before implementing any such project.

D7 Social Media - Protecting Professional Identity

The School has a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party and will be subject to the School's Disciplinary Policies.

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;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk;

School staff should ensure that;

- 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; and
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Any concerns or complaints about the School's use of social media for professional purposes will be passed to the DSL to ensure compliance with the School's policies.

D8 Communication

The official School communication systems may be regarded as safe and secure. Staff and pupils should therefore use only the School services to communicate with others when in school, or on school systems.

Users in receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature must not respond to any such communication and must immediately report it, but not delete the messages, to the DSL (or a deputy) in accordance with the procedure set out in the relevant Anti-bullying Policies.

Any digital communication between staff and pupils or parents (email, Teams 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.

Pupils are provided with individual school email addresses for educational use.

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

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

E. Responding to Online Safety Incidents

E1 Who to report to and how

E.1.1 **ALL concerns, allegations, complaints or suspicions about an online safety incident (illegal or otherwise) should be reported to the relevant DSL** unless that person is the subject of the concern (see E.1.2). Anyone can report an online safety incident - staff, pupils, parents or someone outside the School community.

E.1.2 All concerns, allegations, complaints or suspicions about:

- The DSL should be reported to the Head
- The Head should be reported to the Chair of the Governors; and
- The Chair of Governors should be reported to the Vice Chair

E.1.3 The subsequent course of action is dependent on whether there is any suspicion that the incident is in any way illegal. (See E.2 and Appendix 1).

E2 Illegal Online Safety Incidents

E.2.1 An illegal online safety incident includes where access has been attempted to any web site or materials are found on any electronic device containing:

- child abuse images;
- criminally racist material;
- statements or information intended to radicalize people or incite terrorist activity;
- incidents of online 'grooming' behaviour;
- material that breaches the Obscene Publications Act;
- indecent or explicit images of children, including sharing nudes and semi nudes.

See DfE guidance Searching screening and confiscation at School (for schools) and Sharing nudes and semi-nudes: advice for education settings working with children and young people. **The key consideration is for staff not to view or forward illegal images of a child**; or

- any other suspected illegal activity.

E.2.2 Safeguarding concerns

For any incident with substantial safeguarding concerns of a potentially illegal nature, the DSL will immediately act in accordance with the School's Safeguarding Policy and the most recent version of KCSIE including reporting the concerns to Children's Social Care and the Police. If an allegation is made against a member of staff, the following will also be involved; The CSSP Designated Officer Police, Charity Commission, DBS, or other external agency as appropriate (see Appendix 1).

E.2.3 IT illegal activity

If there is any concern about any IT illegal activity of a member of staff, pupil or parent (such as copyright theft, fraud, or unlicensed software), the DSL will inform the:

- Data Protection Lead if the illegal activity involves a (suspected) data breach; and
- IT Manager who will investigate using activity logs (see E.5 and Appendix 1).

E3 Unsuitable/Inappropriate Online Safety Incidents

E.3.1 Certain activities identified in the Acceptable Use Policies would be unsuitable or inappropriate in a school context and pupils should not engage in these activities in school or outside school when using school equipment or systems, including:

- Using school systems to run a private business;
- Using systems, applications, websites or other mechanisms that deliberately bypass the filtering or other safeguards employed by the School
- Causing a data breach, by revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);
- Infringing copyright;
- Creating or propagating computer viruses or other harmful files;
- Downloading/uploading large files that hinder others use of the Internet (unfair usage);
- Gambling or gaming online
- Shopping online
- Using social media
- Using messaging apps

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

E.3.2 Safeguarding concerns:

Online safety incidents which raise any safeguarding concerns (but do not appear to suggest illegal activity) will be dealt with by the DSL in accordance with the School's Safeguarding Policy

E.3.3 IT concerns;

Reports of misuse of IT equipment or services by members of staff, pupils or visitors will be investigated by the DSL who will liaise with the IT Manager

Misuse detected by, or reported to IT Staff, will be investigated by the IT Manager in the first instance and then referred to the DSL.

E.3.4 Data breach concerns

Reports of any online misuse which caused, or is suspected to have caused, a data breach, should be reported to the Data Protection Lead

E4 Investigating Online Incidents (DSL)

- The DSL will evaluate the incident report to determine the appropriate response and if necessary, initiate an investigation and request the IT staff to investigate in order to establish, capture and preserve any relevant data or other evidence as set out below.
- The DSL will only examine the contents of personal devices not owned by the School in accordance with the procedures set out in the relevant Behaviour Policy.
- Where appropriate, the DSL will consider implementing appropriate sanctions (see Section F below).

E5 Investigating Online Incidents (IT Manager/IT Staff)

When instructed by the DSL, the Head, the Chair of the Governors, the DSL, the police, or other appropriate external agency, the IT Manager/IT staff will undertake the following:

- Examine all technical logs;
- Examine in detail the firewall, filter systems, other will be undertaken;
- Remotely examine the School's desktops and laptops. This is only possible where the computer is turned on and connected to the School network;
- Examine relevant school emails, (including sent and deleted);
- Investigate using a designated computer in the IT Department. There should be two members of staff involved in this process, ideally the IT Manager and the DSL. 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).
- Make a record of the url of any site containing the alleged misuse describing the nature of the content causing concern and unsuitable materials will be copied. 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 or any other indecent images of children– see below)
- Once the incident has been completed and fully investigated, report to the DSL who will 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 in accordance with the School's Behaviour and Anti-bullying Policies (see section F below);
- Police involvement and/or action;
- Report to the Data Protection Lead if the security of personal data has been compromised, who will investigate and consider whether a report to the Information Commissioner's Office is appropriate.

If content being reviewed includes images of child abuse then the monitoring will be halted, the DSL informed and the computer in question will be isolated as best we can. The matter will then be 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, including those produced by children (sexting);
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.
- 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

- Under the direction of the appropriate authority, delete unsuitable materials from the storage, mailboxes or computers in accordance with the procedures set out in the relevant Behaviour Policy.

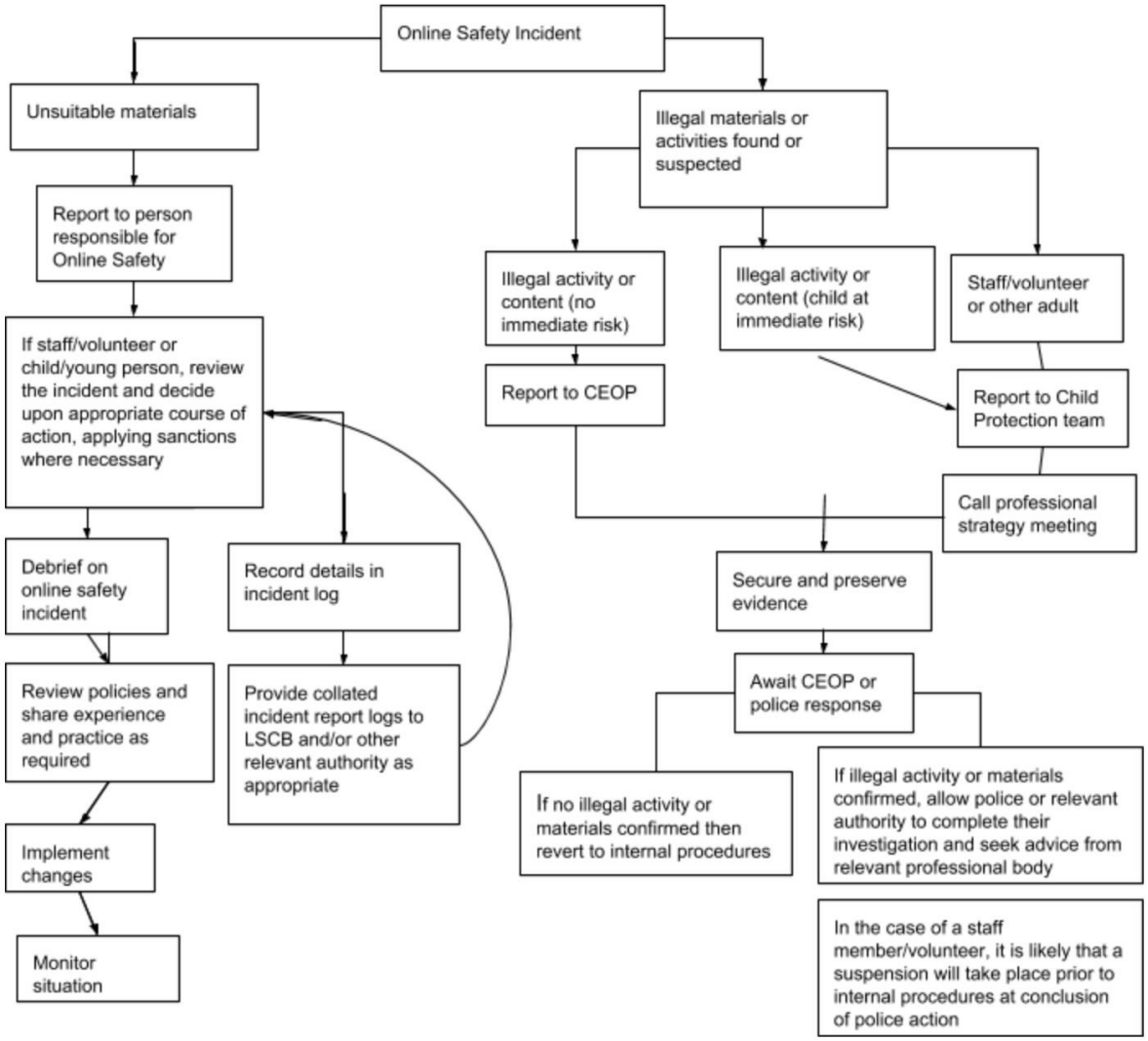
F. Sanctions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal online safety misuse. It is important that any online safety incidents are dealt with as soon as possible in a proportionate manner. Where appropriate, online incidents of misuse by:

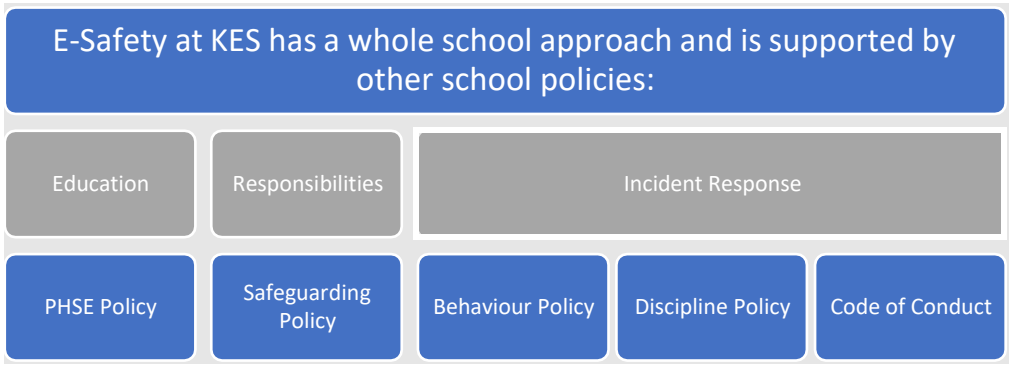
- pupils - will be dealt with through disciplinary procedures set out in the School's Behaviour Policies
- members of staff - will be dealt with through procedures set out in the School's Disciplinary Policies

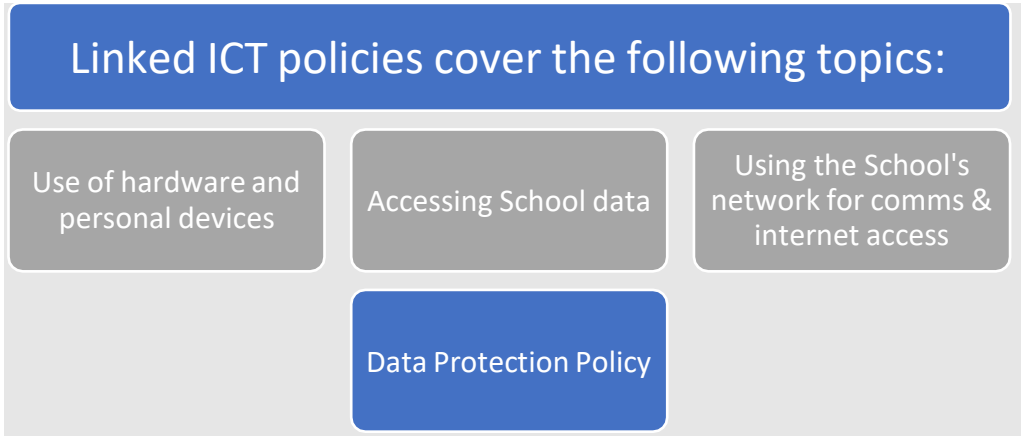
Appendix 1

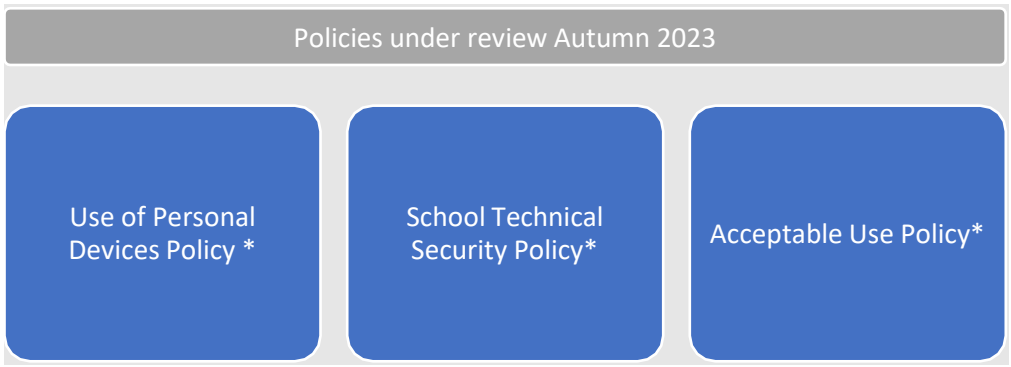
Responding to incidents of misuse- flow chart



Links to other documents







Department for Education (*DfE*)

DfE Meeting Digital and Technology Standards in Schools & Colleges
Teaching online safety in school (June 2019)
Searching screening and confiscation at School (for schools)
Sharing nudes and semi-nudes: advice for education settings working with children and young people. (UKCIS) Dec 2020

Safer Internet Use
Safer Internet Centre -
South West Grid for Learning
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation
INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
Netsmartz http://www.netsmartz.org/index.aspx

CEOP
http://ceop.police.uk/
ThinkUKnow

Support for Schools
SWGfL Digital Literacy & Citizenship curriculum
Insafe - Education Resources

Cyberbullying
DCSF - Cyberbullying guidance
DfE – Preventing & Tackling Bullying
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

Social Networking
Digizen – Social Networking

Data Protection
Information Commissioner's Office

Professional Standards / Staff Training
Revised Safer Working Practice for Adults who Work with Children and Young People
Kent - Safer Practice with Technology
UK Safer Internet Centre Professionals Online Safety Helpline

Working with parents and carers
Get Safe Online - resources for parents
The Digital Universe of Your Children - animated videos for parents (Insafe)

KING EDWARD'S SCHOOL BATH

Appendix B

Summary of objectives of e-safety curriculum

- In Key Stage (KS) 1, pupils will be taught to:
  - Use technology safely and respectfully, keeping personal information private
  - Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Pupils in Key Stage (KS) 2 will be taught to:
  - Use technology safely, respectfully and responsibly
  - Recognise acceptable and unacceptable behaviour
  - Identify a range of ways to report concerns about content and contact
- On leaving the Pre-Prep and Junior School, pupils will know:
  - That people sometimes behave differently online, including by pretending to be someone they are not
  - That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
  - The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
  - How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
  - How information and data is shared and used online
  - What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
  - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Summary of objectives of e-safety curriculum

- In **KS3**, pupils will be taught 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
- Pupils in **KS4** will be taught:
  - To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
  - How to report a range of concerns
- On leaving the Senior School, pupils will know:
  - Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
  - About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
  - Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
  - What to do and where to get support to report material or manage issues online
  - The impact of viewing harmful content
  - That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
  - That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
  - How information and data is generated, collected, shared and used online
  - How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
  - How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)