KING EDWARD VI
SCHOOL LICHFIELD

E-Safety Policy

Ratified by governors:	June 2017
To be reviewed:	June 2020
To be reviewed by:	Assistant Headteacher
Ratified by:	Student & Staff Welfare Committee

Contents **Page**

1.1.1 Aims

- King Edward VI School Lichfield believes that e-safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- The School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- The School has a duty to provide the school community with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the schools management functions. The School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

1.1.2 The purpose of this e-safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the School is a safe and secure environment.
- Safeguard and protect all members of the School's community online.
- Raise awareness with all members of the School's community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.

- Identify clear procedures to use when responding to e-safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour for Learning, Photographic Image Use, Acceptable Use Policies, Freedom of information & data protection, screening, searching & confiscation, and relevant curriculum policies including computing, Sex & relationships.
- This E-safety Policy has been developed by the School, building on SSCB advice with specialist advice and input as required.
- The School has appointed a member of the Governing Body to take lead responsibility for e-safety (e-Safety).
- The School has appointed a member of the Senior Leadership Team as the e-safety lead.
- The School's e-Safety Policy and its implementation will be reviewed at least annually or sooner if required.
- The School's e-Safety Coordinator and Designated Safeguarding Lead (DSL) is Alistair Goodhead, Assistant Headteacher
- The School E-safety lead for the Governing Body is Helen Coulthard

1.2 Key responsibilities of the community

1.2.1 Key responsibilities of SLT are:

- Developing, owning and promoting the e-safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current e-safety practice to identify strengths and areas for improvement.
- Supporting the e-safety lead in the development of an e-safety culture within the school.
- Ensuring there are appropriate and up-to-date policies and procedures regarding e-safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding e-safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that e-safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of e-safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an e-safety culture.
- Taking responsibility for e-safety incidents and liaising with external agencies as appropriate.
- Reviewing e-safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding e-safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of schools systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting e-safety.

1.2.2 Key responsibilities of the designated e-safety lead are:

- Acting as a named point of contact on all e-safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that e-safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school's lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an e-safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school's e-safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating the e-safety policy, Acceptable Use Policy (AUP) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that e-safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor with a lead responsibility for e-safety.

1.2.3 Key responsibilities of staff are:

- Contributing to the development of e-safety policies.
- Reading and the School's AUP and adhering to it.
- Taking responsibility for the security of school/ systems and data.
- Having an awareness of e-safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding e-safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the DSL.
- Knowing when and how to escalate e-safety issues, internally and externally.
- Being able to signpost to appropriate support available for e-safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.2.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the e-safety lead / DSL.
- Ensuring that the use of the School's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the e-safety lead through the ICT link meetings.
- Report any breaches or concerns to the DSL and SLT and together ensure that they are recorded on the e-Safety Incident Log (MyConcern), and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the e-safety lead and SLT, especially in the development and implementation of appropriate e-safety policies and procedures.
- Ensuring that the School's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all users.

1.2.5 Key responsibilities of students are:

- Reading the School's Acceptable Use Policy (AUP) and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing e-safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents and carers are:

- Reading the School's AUP, encouraging their children to adhere to it, and adhering to them themselves where appropriate.
- Discussing e-safety issues with their children, supporting the School in their e-safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the School, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Passing on feedback to support the development of the School's e-safety policy.
- Using the School's systems (including the SWITCH learning platform, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the King Edward VI School website

- The School will ensure that information posted on the School's website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the School's address, email and telephone number. Staff or students' personal information will not be published, unless consent has been given.
- The headteacher will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate.
- The School's website will comply with the School's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Students work will only be published with their permission or that of their parents/carers.
- The administrator account for the School website will be safeguarded with an appropriately strong password.

- The School will post information about safeguarding, including e-safety on the school website.

2.2 Publishing images and videos online

- The School will ensure that all images are used in accordance with the School's Photographic Image Use Policy.
- In line with the School's Photographic Image Policy, written permission from parents or carers will always be obtained on the consent form before images/videos of students are electronically published.

2.3 Managing email

- Students may use school provided email accounts for educational purposes only.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and may be reported to the email provider.
- Any electronic communication that contains any content that could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be. The school-agreed format should be used for such communication.
- Members of the School community must immediately tell a designated member of staff if they receive offensive communication.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- The school has a dedicated email for reporting wellbeing and pastoral issues. studentsupportstaff@kingedwardvi-lichfield.staffs.sch.uk. This inbox is managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Staff should follow the school's e-mail protocol when using school email.

2.5 Appropriate and safe classroom use of the internet and associated devices

- The School's internet access will be designed to enhance and extend education.
- Students will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The School will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All school-owned devices will be used in accordance with the **School's AUP** and with appropriate safety and security measures in place.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- The School will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the School community and exist in order to safeguard both the School and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the School community.
- All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The School will control students and staff access to social media and social networking sites whilst on the school site and using school provided devices and systems.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action.
- Any concerns regarding the online conduct of any member of the School community on social media sites should be reported to the SLT and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding.

3.2 Official use of social media

- Official use of social media sites by the School will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- Members of staff running official school social media channels will follow a specific AUP (Appendix B) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty

to protect private information and will not breach any common law duty of confidentiality, copyright etc.

- Official social media use by the School will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official school social media sites/channels in accordance with the School's Photographic Image Use Policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with approval from SLT.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and students will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- Public communications on behalf of the School will, where possible, be read and agreed by at least one other colleague.
- King Edward VI School Lichfield official social media channels can be found here: http://www.keslichfield.org.uk/?page_id=6175
- An account will link back to the School's website and/or AUP to demonstrate that the account is official.
- The School will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the School, then they are requested to be professional at all times.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the School.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any images posted on the School's social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the School's e-safety (e- Safety) lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via school communication channels.
- Staff using social media officially will agree to the School's social media AUP before official social media use will take place.

3.4 Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the School's Code of Conduct for employees.

- Staff must exercise caution when using information technology and be aware of the risks to themselves and others.
- Where a relationship exists outside of school such as being personal friends with parents of a student, personal online communication is acceptable but caution and professional judgment must be exercised. Staff should consider that all communications may be in the public arena and ensure that they do not compromise themselves or the school. Any communication that raises a concern will be reported to the school's DSL.
- Staff who come in to contact with former students of the school in a personal or professional capacity should exercise reasonable caution. If in doubt, staff are advised to speak to the headteacher or deputy headteacher for advice.
- Staff must exercise caution in the use of internet or social network sites to avoid bringing themselves, the school, school community or employer into disrepute.
- Staff must only use their school email account or school learning platform account when communicating electronically with students, parents and about school matters with colleagues.
- Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with the School's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School.
- Members of staff are encouraged not to identify themselves as employees of the School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.
- Members of staff will ensure that they do not represent their personal views as that of the School on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the School's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

3.5 Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the School's AUP.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and parental consent will be obtained, as required.
- The School is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the School and covered in appropriate policies including the School's AUP, Staff code of conduct, and the Behaviour for Learning policy
- The School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought in to the School are the responsibility of the user at all times. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the behaviour policy.
- All members of the School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School's policies.
- School mobile phones and devices must always be used in accordance with the AUP
- School mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Students use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- For students in Years 7-11, mobile phones and personal devices will be switched off and kept out of sight between morning registration (8.55am) and the end of the school day (3.35pm) except in the circumstances described below.
- Sixth form students may use mobile phones and personal devices in the sixth form common room only during the school day.
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone at an appropriate time. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by a member of staff.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student repeatedly breaches the School's policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school behaviour policy.
- School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the School's behaviour or bullying policy. The phone or device may be searched by a member of staff under the authorisation of the headteacher. Searches of mobile phone or personal devices will be carried out in accordance with the Schools searching, screening and confiscation policy.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the School in a professional capacity. Any pre-existing relationships, which could compromise this, must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff who use their personal mobile phones or tablets to maintain their calendar, check their school email for a specific item (i.e. not routinely) or to take notes should ensure that the use of the device for this purpose is clear should they be in the presence of students.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the School policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be responded to in line with the Safeguarding policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the School's Photographic Image Use Policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

5 Policy Decisions

5.1. Reducing online risks

- The School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the School's Senior Leadership Team (SLT) will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The School will ensure that appropriate filtering systems are in place to prevent staff and students from accessing unsuitable or illegal content.

Our monitoring software will

- Inspect everything that is typed or done
- Will take screen shots and will record any suspicious use detected
- Detect when attempts have been made to access proxy bypass sites
- Help stop downloads of obscene or offensive content
- Potentially get an early warning of predator grooming

- The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The School will audit technology use to establish if the e-safety Policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by SLT.
- Filtering decisions, Internet access and device use by students and staff will be reviewed regularly by SLT.

5.2. Internet use throughout the wider school community

- The School will liaise with local organisations to establish a common approach to e-safety.
- The School will provide an on-screen AUP for any guest/visitor who needs to access the School computer system or internet on site.

5.3 Authorising Internet access

- The School will maintain a current record of all staff and students who are granted access to the School's electronic communications.
- All staff, students and visitors will read and agree to the School's AUP before using any school ICT resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.

- Parents will be asked to read the School's AUP for student access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the School community (such as with children with special education needs) the School will make decisions based on the specific needs and understanding of the student(s).

6 Engagement Approaches

6.1 Engagement and education of children and young people

- An e-safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students' input will be sought when writing and developing school e-safety policies and practices.
- Students will be supported in reading and understanding the School's AUP in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Student instruction regarding responsible and safe use will precede Internet access.
- E-safety will be included in the PSHCE, and Computing/ICT programmes of study covering both safe school and home use.
- The student Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the School's internal e-safety education approaches.
- The School will reward positive use of technology by students.

6.2 Engagement and education of children and young people who are considered to be vulnerable

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

6.3 Engagement and education of staff

- The e-safety Policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- The School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the School's e-safety Policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to e-safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e-safety at other well-attended events e.g. parent evenings and transition events.
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the School's approach to data protection and information governance can be found in the Schools Information Security Policy.

7.2 Security and Management of Information Systems

- The security of the School Information Systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may only be used following an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the School's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The School will log and record internet use on all school owned devices.

7.2.1 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.
- We require staff and students to use STRONG passwords for access into our system.

7.3 Filtering Decisions

- The School's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.

- The School uses educational filtered secure broadband connectivity through RM which is appropriate to the age and requirement of our students.
- The School uses RM Safety Net filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The School will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and students from being accidentally or deliberately exposed to unsuitable content.
- The School will work with the broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The School will have a clear procedure for reporting breaches of filtering which all members of the School community (all staff and all students) will be made aware of.
- If staff or students discover unsuitable sites, the URL will be reported to the School DSL/Network manager and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the School's filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SLT.
- All changes to the School's filtering policy will be logged and recorded.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the School believes is illegal will be reported to appropriate agencies such as IWF, Staffordshire Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Devices will be appropriately secure if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

- All members of the School community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The DSL will be informed of any e-safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that e-safety concerns are escalated and reported to relevant
- agencies in line with the Staffordshire Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's Anti-bullying Policy and procedures
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed between the Headteacher and the LADO (Local Authority Designated Officer).
- Students, parents and staff will be informed of the School's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The School will manage e-safety incidents in accordance with the school behaviour policy where appropriate.
- The School will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Police via 101, or via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- If the School is unsure how to proceed with any incidents of concern, advice will be sought from the Education Safeguarding Advice Service.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Staffordshire
- Parents and children will need to work in partnership with the school to resolve issues.

9 Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

- The School ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating indecent images of children (known as "sexting").
- The School will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
- The School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

- If the School is made aware of incident involving indecent images of a child the School will:

  a. Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Staffordshire Safeguarding Child Boards procedures.
  b. Immediately notify the Designated Safeguarding Lead.
  c. Store the device securely.
  d. Carry out a risk assessment in relation to the children(s) involved.
  e. Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
  f. Make a referral to children's social care and/or the police (as needed/appropriate).
  g. Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  h. Inform parents/carers about the incident and how it is being managed.
  i. Implement appropriate sanctions in accordance with the School's Behaviour Policy but taking care not to further traumatise victims where possible.
  j. Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

- The School will not view the image unless there is a clear need or reason to do so.
- The School will not send, share or save indecent images of children and will not allow or request children to do so.

- If an indecent image has been taken or shared on the school/settings network or devices then the School will take action to block access to all users and isolate the image.
- The School will need to involve or consult the police if images are considered to be illegal.
- The School will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The School will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".
- The School will ensure that all members of the community are aware of sources of support.

9.2. Responding to concerns regarding Online Child Sexual Abuse

- The School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The School will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
- The School's views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Advice Service and/or the Police.
- If the school is made aware of incident involving online child sexual abuse of a child then the School will:

  a. Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Staffordshire Safeguarding Children's Board procedures.
  b. Immediately notify the DSL.
  c. Store any devices involved securely.
  d. Immediately inform the police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form:
  e. http://www.ceop.police.uk/safety-centre/
  f. Where appropriate the School will involve and empower children to report concerns regarding online child sexual abuse.
  g. Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
  h. Make a referral to children's social care (if needed/appropriate).
  i. Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
  j. Inform parents/carers about the incident and how it is being managed.
  k. Review the handling of any incidents to ensure that the school is implementing best practice and the School's SLT will review and update any management procedures where necessary.

- The School will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The School will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If students at other schools are believed to have been targeted then the School will seek support from the Education Safeguarding Advice Service to enable other schools to take appropriate action to safeguard their community.
- The School will ensure that the Click CEOP report button is visible and available to students and other members of the school community, for example including the CEOP report button on the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- The School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The School will take action regarding IIOC regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to IIOC for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the School is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Advice Service and/or the Police.
- If the school/setting are made aware of IIOC then the School will:

    a. Act in accordance with the School's Child Protection and Safeguarding Policy and the relevant Staffordshire Safeguarding Child Boards procedures.
    b. Immediately notify the School's DSL.
    c. Store any devices involved securely.
    d. Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), police via 101 (using 999 if a child is at immediate risk) and/or the Local Authority Designated Office (LADO) (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a student has been inadvertently exposed to IIOC whilst using the internet then the School will:

    a. Ensure that the DSL is informed.
    b. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    c. Ensure that any copies that exist of the image, for example in emails, are deleted.

- If the School are made aware that IIOC have been found on the School's electronic devices then the school will:

    a. Ensure that the DSL is informed.
    b. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    c. Ensure that any copies that exist of the image, for example in emails, are deleted.
    d. Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    e. Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the School are made aware that a member of staff is found in possession of IIOC on their electronic device provided by the School, then the School will:

    a. Ensure that the Headteacher is informed in accordance with the School's whistleblowing procedure.
    b. Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    c. Inform the LADO and other relevant organisations in accordance with the schools managing allegations policy.
    d. Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation or extremism online

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the School's Safeguarding Policy.

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the School's community will not be tolerated. Full details are set out in the school anti-bullying and behaviour policies.
- All incidents of online bullying reported will be recorded.
- These are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Advice Service and/or the Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The School will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
  a. Those involved will be asked to remove any material deemed to be inappropriate or offensive.
  b. A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
  c. Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, **behaviour policy or AUP**.
  d. Parent/carers of students involved in online bullying will be informed.
  e. The Police will be contacted if a criminal offence is suspected.

Appendices

Appendix A – Acceptable Use Policy for Use of the School Network and the Internet

KING EDWARD VI
SCHOOL LICHFIELD

Acceptable Use Policy for Use of the School Network and the Internet

This simplified Acceptable Use Policy (AUP) applies to all members of the school community when using school equipment, both in and out of school hours and when accessing the school network remotely as well as when using it on site. Please read it carefully before signing.

When using the school network and internet you agree to:

- Only access websites that are appropriate for use in school;
- Be careful about what you say to others and how you say it;
- Respect copyright and trademarks. (Remember that you cannot copy material without giving credit to the person or the company that owns it.)
- Be wary before opening e-mail attachments and do all you can to check origins and authenticity;
- Be wary of completing on-line questionnaires or subscription forms;
- Use caution when giving your name, address, telephone number or any other personal information about yourself or about others.

You must not:

- Download games or other programs from the internet;
- Use chat-lines or web-based e-mail services (e.g. Hotmail);
- Send, access or display offensive messages or pictures;
- Use or send bad language;
- Intentionally waste resources thus preventing use by others.

Please note:

- User areas on the school network are carefully monitored and staff may review your files and communications to maintain system integrity.
- Failure to follow this code could result in loss of access to the school network and further disciplinary action may be taken if appropriate
- If applicable, external agencies may be involved in investigating misuse, since certain activities may constitute a criminal offence.

Further detailed information can be found in the school's e-safety policy, located at:
http://www.keslichfield.org.uk/?page_id=330

KING EDWARD VI
SCHOOL LICHFIELD

School Official Social Networking Acceptable Use Policy

For use with staff running official school social media accounts

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety) . I am aware that the (tool using e.g. Facebook, Twitter) is a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (name) and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on (tool using e.g. Facebook, Twitter) and will not be forwarded to any other person or organisation.

5. I will promote online safety (e-Safety) in the use of (tool using e.g. Facebook, Twitter) and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.

6. I will set up a specific account/profile using a school provided email address to administrate the account/site/page (tool using e.g. Facebook, Twitter) and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the (tool using e.g. Facebook, Twitter) site/page/group.

7. Where it believes unauthorised and/or inappropriate use of the (tool using e.g. Facebook, Twitter) or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead urgently.

10. I will ensure that the (tool using e.g. Facebook, Twitter) site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (name) or the head teacher.