KING EDWARD VI HANDSWORTH SCHOOL FOR GIRLS

Digital Safety and Acceptable Use Policy

Document Control

Document Ref:		**Date Implemented:**	March 2020
Version:	1	**Date Modified:**	June 2020 due to Covid-19 school closure
Revision due date:	January 2021		
Governor Committee and date (where applicable)	Welfare Committee 2nd March 2020		
Reviewed by:	Jane Glendenning	**Sign and Date:**	
Authorised by:		**Sign and Date:**	

Related Documents/Policies

Reference	**Title**
	Behaviour for Learning Policy (2019)
	Safeguarding and Child Protection Policy (2019)
	Anti-bullying Policy (2020)
	PSHCE and RSE Policy (2019)
	No Platform for Extremism Policy (2020)
	Bring Your Own Device (Sixth Form) Policy
	Data Protection Policy
	Social Media Policy
	IT Security Policy
	King Edward VI Academy Trust Birmingham digital policies

Guidance - UK online safety laws:
Defamation Act 2013 – makes the website host responsible for removing defamatory material posted to a site.
Education Act 2011 – helps teachers tackle cyberbullying by allowing them to look for and delete inappropriate images or data from electronic devices such as mobile phones.
Criminal Justice and Public Order Act 1994 Section 154 – Section 154 covers all forms of harassment, including written messages.
Malicious Communications Act 1988 - makes it an offence to send a communication with the intention of causing distress or anxiety.

Communications Act 2003 Section 127 – Section 127 makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character. An online groomer may not be covered by this law because they may send messages that aim to build up trust with a child.
Protection from Harassment Act 1997 – covers repeated bullying amounting to harassment.
Serious Crime Act 2015 – the law was passed as part of the Serious Crime Act (2015). It is now formally a criminal offence for an adult to send a sexual message to a child.
Sexual Offences Act 2003 – includes the offence of sexual grooming. But action can only be taken by authorities where it can be proved an adult intended to meet a child.
Protection of Children Act 1978 and the **Criminal Justice Act 1988** – it is illegal for an individual to create, share or possess indecent images or videos of themselves or others who are under 18 years of age.
The Prevent Duty – schools have a statutory duty under section 26 of the Counter Terrorism and Security Act 2015 to identify vulnerable children and young people and prevent them from being drawn into terrorism.

Jane Glendenning (DSL) is responsible for reviewing and updating this procedure.

CONTENTS

Aims and values
King Edward VI Handsworth School for Girls recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence.

> *Technology is central to children's lives. In 2017, just over half of children aged 12 had at least one social media account, despite the minimum age requirements for many sites being 13. By age 13, that figure rises to nearly three-quarters. (Ofcom). Today's children don't see the division between 'online' and 'offline' worlds. Social media is now a ubiquitous part of childhood… (and) is part of the fabric of children's lives. Every moment, every experience is something to be captured online. Posts on social media aren't just a catalogue of 'real' life, they are an integral part of it.*

(How safe are our children? The most comprehensive overview of child protection in the UK. NSPCC 2018)

But whilst using ICT to interact socially and share ideas can benefit everyone in the school community, it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents/carers use it appropriately and practise good digital safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Statement of principles
Digital safety covers the Internet but it also covers mobile phones and other electronic communication technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of digital safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Digital safety is a whole-school issue and responsibility.

Cyberbullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our Behaviour for Learning and Anti-bullying Policies.

To summarise the breadth of issues classified within digital safety is considerable, but can be categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material;
- **Contact**: being subjected to harmful online interaction with other users;
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

Roles and Responsibilities

The Governing Body
Governors are responsible for the approval of the Digital Safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Digital safety falls

within the remit of the governor responsible for Safeguarding. The role of the Digital Safety Governor will include:

- ensure a Digital Safety Policy is in place, reviewed every year and is available to all stakeholders;
- ensure that there is a Digital Safety Coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive;
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to; and
- hold the Headmistress and staff accountable for digital safety.

Headmistress and Senior Leadership Team (SLT)

The Headmistress has a duty of care for ensuring the safety (including digital safety) of members of the school community, though the day-to-day responsibility for digital safety will be delegated to the Digital Safety Coordinator. Any complaint about staff misuse must be referred to the Digital Safety Coordinator at the school or, in the case of a serious complaint, to the Headmistress.

- The Headmistress is responsible for ensuring that the Digital Safety Coordinator receives suitable training to enable them to carry out their digital safety roles and to train other colleagues, as relevant.
- The Headmistress will ensure that there is a Digital Safety Policy, Staff Code of Conduct and an IT Security Policy, in place within the school covering usage by teaching and technical staff, and pupils.
- The Headmistress should be aware of the procedures to be followed in the event of a serious digital safety allegation being made against a member of staff.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT (Mrs Kendall, Deputy Head.)
- Ensure that student or staff personal data as recorded within the School Information Management system sent over the Internet is secured.
- Work in partnership with the Department for Education (DfE) and the Internet Service Provider and school Network Manager to ensure systems to protect students are reviewed and improved.
- Ensure the School ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Leadership Team will receive monitoring reports from the Digital Safety Coordinator.

Digital Safety Coordinator (Mrs Kendall):

- Leads Digital Safety meetings.
- Works in partnership with the DfE and the Internet Service Provider and school Network Manager to ensure systems to protect students are reviewed and improved.
- Ensures the school network system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Reports to Senior Leadership Team.
- Liaises with the Designated Safeguarding Lead, nominated member of the governing body & Headmistress to provide an annual report on digital safety.

Designated Safeguarding Lead (DSL) (Miss Glendenning):

The DSL should be trained in Digital Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate digital contact with strangers, incidents of grooming and cyberbullying.

The DSL will discuss current issues with the Senior Leadership Team, Pastoral Leaders (PLs) and members of the Digital Safety Group (including Subject Leads for Computing and PSHCE). The DSL will work with the PLs to decide how incidents should be dealt with; what investigation will be required and what sanctions will be applied (see Behaviour for Learning and Anti-bullying policies).

The DSL will receive Smoothwall reports of digital safety incidents and create a log of incidents to be shared with SLT and PLs and to inform future digital safety developments.

The DSL will liaise with the Digital Safety Coordinator and report to Senior Leadership Team and the Welfare Committee.

The DSL will also: provide regular updates for parents; provide opportunities for parents to attend workshops on digital safety; produce digital safety bulletins for staff and students as part of the weekly safeguarding updates; and train staff on preventative digital safeguarding measures.

Network Manager/Technical Staff:
The Network Manager is responsible for ensuring:

- That the School's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the School meets required digital safety technical requirements and any relevant body digital safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with digital safety technical information in order to effectively carry out their digital safety role and to inform and update others as relevant.
- That the use of the network/Internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Digital Safety Coordinator and DSL for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

The School community
Students, staff and parents are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff, students and parents to remember that they are representing the School community at all times and must act appropriately.

Parents and carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings/workshops, newsletters, School Comms weekly bulletins, school website (with links to ParentZone) and information about digital safety campaigns etc.

Outside school, parents bear the same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, films, radio and other media.

Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home. In addition, if there is a period of school closure which necessitates the wider use of video/audio conferencing to supplement or deliver teaching and learning, students, staff and parents still need to hold to the principles of this policy and usual sanctions will apply.

Based on a representative sample of children in the UK in 2017, Ofcom round that 12-15 year olds spend an average 20 hours 48 minutes online each week. 24% of young people have experienced an adult they don't know in real life trying to contact them online. Despite the common perception that online abuse is less impactful, NSPCC research has shown that the impact of 'online' and 'offline' abuse is the same. Children who have been subjected to online abuse have reported a range of negative experiences, which can include: flashbacks; depression; self-harm; anxiety; and self-blame. The impact of losing control of an image can be particularly damaging for young people, as they know the images could be shared or re-viewed at any time without their permission. Therefore, parents should be encouraged to:

- discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- get to know the sites their children visit, and talk to them about what they are learning;
- ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details;
- ensure that electronic devices are not used in private spaces in the home. Messages which can be exchanged at night, out of sight of parents and carers, can build feelings of secrecy and intimacy in exploitative relationships. The Police advise that electronic devices are not used in young people's bedrooms and that they are stored/charged overnight in parent/carer's bedrooms;
- support the message given by the school to their daughters not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images.

Any unacceptable use of the Internet outside of school should be reported to the Police who can investigate IP addresses and malicious content.

If you're worried that your child is being groomed online or sexually exploited you should report your concerns to CEOP. www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/

It is not always easy to spot the signs of online grooming and sexual exploitation so if you have any concern at all about someone your child is in contact with, you should get in touch. You should always report if your child is or has been in contact with someone who is:

- Chatting online to your child about sex;
- Asking them to do sexual things on webcam;
- Asking to meet up if they've only met them online;
- Requesting sexual pictures;
- Forcing them into sexual activity;
- Making them feel unsafe.

CEOP is a command of the National Crime Agency and can investigate what is happening – with the assurance that the safety and wellbeing of your child is paramount at all times. **If you are concerned that your child is in immediate danger, call 999.**

You can make a report to CEOP using the www.ceop.police.uk/safety-centre. You will need to complete an online form which will ask you for your contact details and information about what has happened. It will ask:

- What happened?
- Who did it happen to?

- What do you know about the suspect involved?

You should complete the form as fully as you can but don't worry if you don't have all of the details. If you want to discuss your concerns with someone first then call the NSPCC Helpline on 0800 800 5000.

All of the reports are first reviewed by child protection social workers. They will:

- Read the report and assess the risk to your child;
- Look to make contact with you to discuss next steps;
- Give safeguarding advice and support.

It is important to remember that it can be difficult for a child to come forward and tell an adult what has happened to them – they are often embarrassed, fear adults won't understand, scared they will get into trouble or that adults will over react. Ensure you tell your child that whatever has happened, it is not their fault and you are on their side.

Further resources are available through the links in Annex A.

Students

Students are responsible for using the school digital technology systems in accordance with an Acceptable Use Agreement and to have a good understanding of research skills so as to avoid accessing unsuitable sites.

In a free society, there is understandably little regulation of 'social' activity however it is important to remember to:

- Keep personal information private. Do not hand out any personal details over the Internet such as mobile phone numbers or email addresses.
- Consider the long-term implications of content posted digitally.
- Not post inappropriate, offensive or illegal content to your own or other digital spaces.
- Not respond to any messages which are inappropriate or rude.
- Use netiquette – being polite to others digitally in the same way you would offline.
- Not open messages from someone you don't know.
- Not send messages when angry.
- Adhere to any website's terms of use – including age restrictions.
- Think carefully about the timing of any messages and its affect on the recipients work/life balance. Consider using schedule send and adhering to office hours for staff communications which should only be via the school email system.

Another guiding principle should be that real-life social rules are the best analogy for understanding the opportunities and risks of social media for example, staff and students are not 'friends'.

It is important that students understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. It is expected that students will:

- Understand the importance of adopting good digital safety practice in and out of school;
- Avoid and report any incidents of cyberbullying;
- Understand policies on the taking/using of images;
- Be expected to safely use all mobile devices and digital camera technology.

In addition, if there is a period of school closure which necessitates the wider use of video/audio conferencing to supplement or deliver teaching and learning, students, staff and parents still need to hold to the principles of this policy and usual sanctions will apply.

Staff (E-safetySupport.com)

Follow the DfE Teacher Standards and:

- Be professional on the Internet – including Facebook, Twitter and any other social media networks.
- Don't post anything inappropriate, including comments or photos which might embarrass yourself or the School.
- Avoid interacting with, initiating contact with or "friending" current pupils using your personal profile.
- Keep all school-related conversations focused on school, teaching and learning.
- Remember, there is potential for anything you post online to be copied and distributed. Bear this in mind every time you post.
- Check – are you able to delete the content once you have posted it? How long will the material stay online? Consider your digital footprint.
- Always ensure you own the rights to your content. Posting someone else's copyrighted material will appear very unprofessional if a complaint is made.
- If you intend to use social media as part of your teaching, ensure parents and other teachers are clearly briefed on how this will work. Seek and obtain written permissions if required.

Advice from Alan Newland, advisor to the DfE and the GTC. YouTube – newteacherstalk

- Be clear about you and your purpose: if you want to share ideas, resources, interests with other teachers, use keywords in your profile: 'I'm a SENCO at a primary school in York, looking to share all things techy';
- Use appropriate photos: one that shows you, not you and your friends, your husband or your dog – just a nice picture of you smiling;
- Find your audience: source like-minded people, like other teachers, whose interests you are likely to share and whom you can trust;
- Protect passwords and security: change them regularly, cancel auto log-ins and 'remember me' functions;
- Keep your 'followers', friends' and 'connections' under review and cull them regularly;
- Maintain 'private' profiles or set them to allow only 'invited' or those 'approved' to your network;
- Ask friends and family not to 'tag' you in ways that may compromise your professional persona;
- 'Pause before you post': ask yourself: 'How would I feel about this if I was a parent of a pupil at my school?'
- Follow the school rules: employers have a right to expect that networking isn't a distraction from your job or a reputational risk.
- In the appropriate context, model good social media behaviour to your students in the way you would model your real-life relationships – with mutual respect, due consideration for privacy and personal boundaries.

Communicating the Digital Safety and Acceptable Use Policy

This policy is available on the school website for parents/carers, staff, and students to access when and as they wish. Digital safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHCE lessons as part of the 'Economic wellbeing and The Digital World' strand where personal safety, responsibility, and the law are being discussed.

Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions.

Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. In a time of extended school closure the use of shared school platforms such as Google Classroom will be utilised to progress learning and to monitor student progress, alongside the potential use of real time conferencing via Google Meets staff to student, or staff to staff via Google meets, teams or zoom. (At this time only Google Meet is operated by the school). Additional protocols will be issued to staff and students to support the use of these remote learning tools.

Some of the benefits of using ICT and the Internet in schools are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations. The Internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents/carers.
- Class management, attendance records, schedule, and assignment tracking.

Learning to evaluate Internet content

With so much information available online it is important that students learn how to evaluate Internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- Use age-appropriate tools to search for information digitally;
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the School will take any intentional acts of plagiary very seriously (see *Sanctions* appendix in the Behaviour for Learning Policy). Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the School Digital Safety Coordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Examples of unacceptable use of the Internet

- Searching, viewing, and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- Copying, saving and/or redistributing copyright protected material, without approval;
- Subscribing to any services or ordering any goods or services, unless specifically approved by the School;
- Playing computer games or using other interactive 'chat' or social networking sites in lessons, unless specifically assigned by the teacher;
- Using the network in such a way that use of the network by other users is disrupted, for example downloading large files during peak usage times or listening or watching streamed video and music;
- Publishing, sharing or distributing any personal information about a user (such as: home address, email address, phone number etc.);
- Activities that threaten the integrity of the School ICT systems, or activity that attacks or corrupts other systems is forbidden; and
- Any activity that violates a school rule.

Managing Information Systems

The School is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our School community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Technicians/Network Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted;
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this;
- Files held on the school network will be regularly checked for viruses. Anti-virus software is installed on all computers and updated regularly;
- The use of user logins and passwords to access the school network will be enforced;
- Laptops used to transport school data must be encrypted;
- Central filtering is provided and managed by ICT Systems. All staff and students understand that if an inappropriate site is discovered it must be reported to the IT Technical Team;
- Requests for changes to the filtering will be directed to the Network Manager who will liaise with the Digital Safety Coordinator as appropriate;
- the school uses Smoothwall, Impero and Visigo on all school owned equipment to ensure compliance with relevant policies;
- Students' use is monitored by the DSL/Deputy DSLs and Digital Safety Coordinator;
- Staff use is monitored by the Headmistress and the IT Technical Team;
- All staff are issued with their own username and password for network access and understand that this must not be shared. Visitors/supply staff are issued with temporary ID's and the details recorded by the IT Technical Team; and
- All students are issued with their own username and password and understand that this must not be shared.

For more information on data protection in school please refer to our Data Protection Policy on the school website/Moodle.

Emails

The school uses email internally for staff and students, and externally for contacting parents/carers, and is an essential part of school communication.

Staff and students should be aware that school email accounts should only be used for school-related matters, i.e. for Form Tutors, Subject Teachers, Pastoral Leaders or members of the SLT to contact parents/carers, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

School Email Accounts and Appropriate Use
The School does not assign school email addresses that state students' full names as this makes them more vulnerable to being identified by unsuitable people. Email accounts in school are only allowed to be those that have been managed and approved by the School.

Staff:
Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with students, parents/carers. Personal email accounts should not be used to contact any of these people and should not be accessed during teaching? hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their Line Manager or a member of the SLT if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.
- Please use the schedule send facility to avoid impacting student and staff work/life balance out of normal office hours, this includes at weekends or during holidays.

Students:
Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the curriculum and in any instance where email is being used within the curriculum or in class:

- In school, students should only use school-approved email accounts.
- Social emailing is not permitted.
- Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Students must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from their parent.
- Please use the schedule send facility to avoid impacting student and staff work/life balance out of normal office hours, this includes at weekends or during holidays.

Students will be educated through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Parents/carers
The School will communicate to parents/carers over email and text message through a system called School Comms. It's parents' responsibility to ensure that their child does not have access to this account.

School will use this system to:

- Advise you if your daughter needs to be picked up due to illness or accident;
- Advise you if your daughter has not arrived in school or of other attendance concern;
- Provide information e.g. snow closures;
- Issue letters and newsletters;
- Provide attainment and progress reports.

For this system to work smoothly, please keep us informed of any changes to your home, mobile or email contact details.

Parents should communicate academic concerns via email to Subject Teachers in the first instance. Any generic concerns around physical and emotional wellbeing should be communicated to Form Tutors who will escalate to Pastoral Leaders if necessary.

Parents are encouraged to email the DSL if there is a change in home circumstances that will impact on their daughter.

Please use the schedule send facility to avoid impacting staff work/life balance out of normal office hours, this includes at weekends or during holidays unless it is an emergency. Be aware that staff are not routinely monitoring their emails out of office hours.

Published Content and the School Website
The school website is viewed as a useful tool for communicating our School ethos and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office only.

The school has a Twitter account which is monitored by Mrs Daniel, Assistant Head and Deputy DSL and all communication is subject to her approval. Official school Twitter accounts created by staff/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.

Policy and Guidance of Safe Use of Children's Photographs and Work (see Annex D)
Colour photographs and students' work bring our school to life, showcase our students' talents, and add interest to publications both digital and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or digitally, without consent. On admission to the school, parents/carers will be asked to sign a photography consent form. The School does this so as to prevent repeatedly asking parents/carers for consent over the school year, which is time-consuming for both parents/carers and the School. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the School will be used in public and children may not be approached or photographed while in school or doing school activities without the School's permission. The School follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
    - all school publications;
    - on the school website;
    - in newspapers as allowed by the School;
    - in videos made by the School or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the student.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse will focus more on the sport than the students.
- For public documents, including in newspapers, full names will not be published alongside images of the student. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to our School Safeguarding Policy.

Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedures if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the School' Safeguarding and Child Protection Policy and Behaviour for Learning Policy.

Our students increasingly use electronic equipment on a daily basis to access the Internet and share content and images via social networking sites such as Twitter, MSN, Tumblr, Tik Tok, Snapchat and Instagram.

Unfortunately, some adults and young people will use these technologies to harm others. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Students may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Cyberbullying and sexting by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our Safeguarding and Child Protection Policy.

Many students own or have access to hand held devices and parents are encouraged to consider measures to keep their children safe when using the Internet and social media at home and in the community (see Annex A links for up-to-the-minute advice).

All staff are responsible for ensuring they understand and follow School policy and procedures in relation to digital safety.

Educating students about social networking, social media and personal publishing

Personal publishing tools include: blogs; wikis; social networking sites; bulletin boards; chat rooms; and instant messaging programmes. These digital forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct digital.

- Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the Computing and PSHCE curriculum, and assemblies/form time activities about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.
- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

Mobile Phones and Personal Device (page 8 of pupil planners)

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make students and staff more vulnerable to cyberbullying;
- Can be used to access inappropriate Internet material;
- Can be a distraction in the classroom;
- Are valuable items that could be stolen, damaged, or lost;
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

In order to minimise the risk of misuse of personal devices and to support our Behaviour for Learning, Anti-bullying and Safeguarding and Child Protection Policies, it is against school policy for Yr 7 – 11 pupils to have mobile phones on their person during the school day. KS3 and 4 students' mobile phones should be secured in students' locked locker as soon as they arrive in school and

collected at the end of the day. KS5 students must keep their mobile phones turned off during lesson times and kept safely in their school bags. Sanctions will be imposed if students fail to follow this rule. The only exception is at the specific request of a member of staff to aid teaching learning in a supervised classroom.
If a student is seen with their phone/ear phones at any time on the school premises before 3.35 pm, the phone/ear phones will be confiscated and handed in (by the member of staff) to Reception. Parents will be informed by the relevant Pastoral Leader. The student will then need to hand in their mobile phone/ear phones to Reception at the start of each day and collect at the end of the day for 5 days.

If students are seen with their phone/ear phones again, the School will take the above steps but the student will also be in a half hour after school Tuesday detention set by their Pastoral Leader. The next escalation stage is that they will be in an hour SLT Thursday detention set by their Pastoral Leader. On this occasion parents will be asked to collect the phone after school on Friday after at least 5 days of confiscation.

Mobile Phone or Personal Device Misuse

- The School will not tolerate cyberbullying against either students or staff.
- Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.
- Images or files should not be sent between mobile phones in school.

Any member of staff can confiscate mobile phones, and a member of the SLT or Pastoral Team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device. (See Behaviour for Learning Policy and searching with/without consent.) In the event of a student not unlocking the device it will be secured until a parent can be present to view the search.

Students

- Students who breach school policy relating to the use of personal devices will be disciplined in line with the School's Behaviour for Learning policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal electronic devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

Staff

- Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The School expects staff to lead by example. Staff may have personal mobile phones in their classroom in case of emergencies, however, mobile phones should be on 'silent' during lesson times.
- If staff wish to use these personal devices in class as part of a learning project, they must get permission from their Senior Leadership Subject Link and ensure that they have carefully laid the ground rules with the students in advance
- Any breach of school policy may result in disciplinary action against that member of staff.

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The School keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting Personal Data

King Edward VI Handsworth School for Girls believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The School collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 2018, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed;
- Process data only for limited purposes;
- Ensure that all data processed is adequate, relevant and not excessive;
- Ensure that data processed is accurate;
- Not keep data longer than is necessary;
- Process the data in accordance with the data subject's rights;
- Ensure that data is secure;
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the School’s safeguarding procedures relating to data protection read the School’s Data Protection Policy.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour for Learning, Anti-bullying and Safeguarding and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Schools of King Edward VI Foundation Office will be informed to ensure that they provide appropriate support for the School.
- If parents need to inform the Police of any inappropriate online activity that occurs outside the normal school day, the Digital Safety Coordinator needs to be informed for our reference.
- Breaches of this policy by staff will be investigated by the Headmistress. Action will be taken under the Foundation’s Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least two senior members of staff.

- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with the School Behaviour for Learning Policy. Referral to PLs will be appropriate at this level. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor student offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the School Behaviour for Learning Policy.
- The Educations and Inspections Act 2006 grants the Headmistress the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

Steps for teachers to avoid becoming victims of online abuse
Education boards and legislatures are recognising that teachers with social networking profiles are vulnerable to online abuse. Female teachers are a particular target, according to the Scottish Secondary Teachers' Association which has detailed how bad behaviour has spread from the classroom to abusive behaviour on the Internet.

What to do if you are contacted via your personal social media account:

- If a student sends you a message and you think it is inappropriate to respond, respond to it in real life, not via the Internet.
- Consider creating a standard cut and past response, for example, "I'm sorry I cannot reply to your message using my personal Facebook/Twitter – I will reply via official school email/letter or in person at school".
- Do consider blocking students and parents who you think might be abusive even pre-emptively, but don't use personal data held by the school under the Data Protection Act (for example email addresses) to track them down online.

If there are concerns about members of the School community and online safety issues, the DSL or Digital Safety Coordinator will contact The Professionals Online Safety Helpline (POSH) on 0344 381 4772 or via helpline@saferinternet.org.uk Monday to Friday 10am - 4pm and seek advice.

As the only helpline in the UK solely dedicated to supporting the children's workforce, POSH offer free and independent advice on any number of online safety issues, including: privacy, online reputation, gaming, grooming, cyberbullying, sexting, inappropriate behaviour on social media etc. They have relationships with industry which includes direct channels to escalate concerns to social media companies and many websites.

ANNEX A: useful links

Students
Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 1111 or in an online chat at www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx

www.childline.org.uk/info-advice/bullying-abuse-safety/digital-mobile-safety/sexting/ - Childline support on sexting

https://www.ditchthelabel.org/living-insta-lie/ - an amusing reminder about social media v reality.

Zipit – app allowing young people to send humorous responses to anybody who has asked them to send an explicit image.

Parents

www.bbc.com/ownit/take-control/own-it-app The Own It app comes with a special keyboard. This can be used like any other keyboard, but it also gives your child helpful tips and friendly advice as they write!

- Track how they feel and improve their wellbeing.
- Packed full of gifs and emojis to help them express themselves!
- Lots of fun quizzes, videos and articles to enjoy.

www.nspcc.org.uk/keeping-children-safe/digital-safety/ - whether you're a digital expert or you're not sure where to start, the NSPCC's tools and advice will help you keep your child safe.

www.saferInternet.org.uk - where you can find e-safety tips, advice and resources to help children and young people stay safe digital.

http://jcoleman.co.uk/wp-content/uploads/2019/01/SocialMedia.pdf - Social media and teenagers. A practical approach. A guide from The Charlie Waller Memorial Trust.

www.commonsensemedia.org – to learn more about the games or apps your children are using, Common Sense Media covers thousands, which includes advice and reviews from other parents.

www.thinkuknow.co.uk/parents/articles - advice and information for parents, including link to report a concern.

www.Internetmatters.org – helping parents keep their children safe digital.

www.net-aware.org.uk – online guide to the social networks, sites and apps children use.

www.childnet.com - non-profit organisation working with others to help make the Internet a great and safe place for children.

www.iwf.org.uk – Internet Watch Foundation receive, assess and trace public complaints about child sexual abuse content on the internet and support the development of website rating systems. It is also the UK hotline for reporting criminal online content with particular reference to images of child sexual abuse.

http://parentinfo.org/article/where-do-i-report-if-im-worried-about-my-childs-safety-digital - a parent's guide to help report digital activity.

www.parentsprotect.co.uk – provides information and resources for parents about chld sexual abuse, including a section on online safety.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf - Child Safety Digital: A practical guide for parents and carers whose children are using social media.

www.snapchat.com/l/en-gb/safety/ and www.parentinfo.org/article/snapchat-what-to-do-if-you-re-worried - Snapchat digital safety.

www.lifewire.com/what-is-instagram-3486316 - what is Instagram and how is it used?

www.lifewire.com/what-is-snapchat-3485908 - what is snapchat and how is it used?

www.connectsafely.org/a-parents-guide-to-mobile-phones - a parent's guide including tips for Smartphone use; helping children protect their safety, privacy and security; and parental controls.

www.connectsafely.org/wp-content/uploads/A-Parent's-Guide-to-Snapchat.pdf - a parent's guide to Snapchat (US version). Note UK support address on page 5 is: https://support.snapchat.com/en-GB/i-need-help

http://www.connectsafely.org/familylink/ - this guide provides parents with an overview of the Family Link parental tools with tips on how to set up and manage their child's device, including setting "screen time" to determine how long and at what times they can use their device.

www.connectsafely.org/fakenews - a parent and educator guide to media literacy and fake news.

www.childrenscommissioner.gov.uk/publication/life-in-likes/ This Children's Commissioner's report on the effects of social media on 8-to-12-year-olds examines the way children use social media and its effects on their wellbeing. 'Life in Likes' fills a gap in research showing how younger children use platforms which social media companies say are not designed for them.

www.esafety-adviser.com/latest-newsletter/ - teachers or parents can sign up to the newsletter which comes out every 6 weeks.

www.bps.org.uk/news-and-policy/changing-behaviour-children-adolescents-and-screen-use Interesting paper from the British Psychological Society (2018). The recommendations set out in the paper recognise that the issue of children's digital media use is more complex than amount of screen time and acknowledges both benefits and risks to media use.

Staff

https://digital-literacy.org.uk/ South West Grid for Learning provide free materials designed to empower students to think critically, behave safely, and participate responsibly in our digital world. Browse by Key Stage or Year Group, for cross-curricular lessons which address digital literacy and citizenship topics in an age-appropriate way.

www.gov.uk/government/publications/education-for-a-connected-world The Education for a Connected World framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis The UK Council for Child Internet Safety is now the UK Council for Internet Safety (UKCIS)

www.gov.uk/government/publications/teaching-online-safety-in-schools 2019 guidance supporting schools to teach pupils how to stay safe online when studying new and existing subjects.

www.ofcom.org.uk/__data/assets/pdf_file/0024/149253/online-nation-summary.pdf - Online Nation is a new annual report that looks at what people are doing online, how they are served by online content providers and platforms, and their attitudes to and experiences of using the internet. It brings the relevant research into a single place and aims to act as a data- and insight driven resource for stakeholders at a time of significant evolution in the online landscape.

www.e-safetysupport.com/resources/details/?resource_type=support_advice – what every teacher needs to know about e-safety.

https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf -this study looks at a number of vulnerable groups in order to ascertain differences of experiences and vulnerabilities.

www.rsph.org.uk/our-work/policy/wellbeing/new-filters.html - the All Party Parliamentary Group (APPG) on Social Media's report on the Group's Inquiry, "#NewFilters to manage the impact of social media on young people's mental health and wellbeing". This is the first national Inquiry specifically examining the impact of social media on the mental health and wellbeing of young people, which ran from April 2018 to January 2019.

www.thinkuknow.co.uk/professionals/ - supporting you to deliver education and raise awareness of digital child exploitation and abuse.

www.thinkuknow.co.uk/professionals/guidance/digital-romance/ This research project looks at how young people use technology in developing romantic relationships and surviving break ups. The project was led by Brook, the UK's leading sexual health and wellbeing charity for under 25s, and the CEOP Command of the NCA.

www.tes.com/teaching-resource/digital-citizenship-young-peoples-rights-on-social-media-teaching-pack-for-11-14-year-olds-11734349 **Digital citizenship: Young peoples' rights on social media** - Teaching pack designed to help students aged 11 to 14 develop the resilience, power and information they need to thrive online, this teaching pack comprises: a short, six-lesson unit of work written by teacher and citizenship specialist Emily Cotterill.

www.nen.gov.uk/digital-safety - leading educational support for helping you stay safe digital.

https://educateagainsthate.com/ - This website gives teachers, parents and school leaders practical advice and information on protecting children from extremism and radicalisation.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf - this briefing note is aimed at head teachers, teachers and safeguarding leads and provides advice about digital terrorist and extremist material.

www.mercurynews.com/2017/09/21/how-to-combat-lgbtq-cyberbullying - article on combating LGBTQ+ bullying.

https://www.barnardos.org.uk/campaign-with-us/childrens-social-media-and-mental-health report

https://www.gov.uk/government/publications/sexting-in-schools-and-colleges 'sexting' in schools: advice and support around self-generated images. This advice is for designated safeguarding leads (DSLs), their deputies, head teachers and senior leadership teams in schools and educational establishments.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf - Children's digital activities, risks and safety. A literature review by the UKCCIS (UK Council for Child Internet Safety) Evidence Group. October 2017.

https://www.gov.uk/government/publications/digital-resilience-framework A framework and tool for organisations, policymakers, schools and companies to use to embed digital resilience thinking into products, education and services.

The NSPCC Knowledge and Information Services provide newsletters and updates on safeguarding research, including digital safety. Information can be found at www.nspcc.org.uk/library CASPAR (Current Awareness Service for Policy, Practice and Research is the NSPCC's weekly email update delivering the latest news in child protection policy, practice and research, every Monday. Sign up to CASPAR at www.nspcc.org.uk/caspar or you can follow them on Twitter @NSPCCpro The NSPCC also provide specialist child protection courses (introductory, advanced and specialist) either online or face-to-face www.nspcc.org.uk/training

ANNEX B: Managing your digital footprint – Alan Mackenzie

Everything we do digital contributes to a 'digital footprint' that can be traced, profiled or even compromised – by Alan Mackenzie. (For 7 years Alan Mackenzie was the Service Manager at Lincolnshire County Council managing all IT services for around 350 schools as well as being the e-safety lead for Children's Services raising initiatives for schools, police.)

What is a digital footprint?

'One's unique set of digital activities, actions and communications that leave a data trace on the Internet, or on a computer or other digital device and can identify the particular user or device.'

Our digital footprint can be split into two categories: passive and active.

Passive digital footprint

How long we watch a Facebook video, what we shop for and what we search on Google are all examples of our passive digital footprint.

These are mainly convenient snippets of code used to store information not only on our own devices, but also in the 'cloud' (shared storage space) as well. It's becoming more common for companies to use computer algorithms to profile us individually, and tailor things for us. The longer you watch a Facebook video, the more interested you must be, therefore you'll see more similar content.

Another more common example is targeted advertising. If I've been looking at something on Amazon, I soon find adverts for similar items across my Instagram timeline and when I'm browsing the web. It's marketing on a grand scale, and many companies sell and share our personal information with each other. We give companies permission to do this when we sign up for and use their services.

Many companies sell and share our personal information with each other
Similarly, details about our habits are recorded when we're in a shop, commonly called 'location-based engagement'.

This data used to be stored locally on the device itself, but as many of us have become owners and users of multiple devices, these details are also stored elsewhere for convenience.

For example, if I use the Google Chrome browser at home and allow it to store all my login details (or perish the thought, banking details), I can easily sign into my Google account from a computer or device anywhere in the world, as if I were sat at home.

Active digital footprint

An active digital footprint mainly describes what we are deliberately (or sometimes accidentally) sharing digital. Examples include:

- an email;
- a Facebook post or share;
- a photo shared on Instagram;
- a 'like' on a YouTube video; or
- a typed comment on an digital game.

The consequences of a poorly-managed digital footprint primarily fall into four categories: reputation, legality, university and employment. In other words, carelessness (deliberate or inadvertent) can have repercussions for someone's reputation and life chances in the present or years to come. For example the story of Paris Brown.

Nothing we do or say digital is truly confidential. Privacy affects every single one of us. Privacy settings are great in principle, but they're no guarantee of safety.

26 APR 2017

ANNEX C: Sexting: get your facts straight – Dai Durbridge

Sharing images digital is a natural part of most children and young people's lives, but sexting has legal consequences. Understand how the law applies, and how you can get the message across. (Dai Durbridge is a Partner in the education team at Browne Jacobson solicitors and specialises in safeguarding. Dai provides advice and training to teachers and other education professionals on relevant legal and practical issues.)

When sending images across social media is normal activity in most pupil's lives, there is no point in schools trying to discourage it. What is important, however, is knowing what is acceptable, not just in terms of behaviour and safety, but legally as well.

There are various social media channels that pupils may use:

- Snapchat
- Instagram
- WhatsApp
- Viber

What the law says

Creating or sharing indecent images of a child is illegal, even if it is a child doing it. A young person will be breaking the law if they take an explicit photo of themselves or a friend, share an explicit photo or video of a child (even if it is shared with other children) or possess such an image or video of a child, even if that child consents.

Whilst convictions are rare where children share with other children consensually, the police can now decide to record the action as a crime but also decide that taking action is not in the public interest.

Based on current law, it is unlikely that a crime recorded in this way would appear on a future DBS check when the child is an adult. However, given the continuing changes in this area of law, the position may well be different in 10 or 15 years' time.

A child is someone under the age of 18 – this was changed from 16 in the Sexual Offences Act 2003. According to the Protection of Children Act 1978, it is an offence:

- **to take, permit to be taken, or to make** any indecent photographs or pseudo-photographs of a child;
- **to distribute or show** such indecent photographs or pseudo-photographs;
- **to have in his possession** such indecent photographs or pseudo-photographs **with a view to their being distributed or shown by himself or others**.

- If a pupil sends an indecent image or video of themselves and posts it on social media and they are under 18, it could count as distributing an indecent image of a child and could result in police action.
- It makes no difference if the image or video is of themselves or someone else the same age.
- It is illegal for anyone under 16 to have sex, therefore sending an image or video of a sexual act is likely to be viewed as more serious than sending an indecent image or video.
- If a pupil aged 17 sent an image or video of themselves performing a sexual act, they would still be guilty of distributing an indecent image or video of a child, but not breaking the law about consensual sex. However, a 15 year old would be committing both offences.
- If a pupil sends an indecent image or video to someone who finds the image upsetting and didn't want to see it, that could be a crime under the Malicious Communications Act 1988.

- Outside of criminal law, there are also civil law remedies available to individuals of whom images or video have been shared. This could include breaching copyright and privacy.
- You can also be prosecuted if you are found to have shared a sexual image for 'revenge porn' purposes.
- If you're over 18 and someone's shared a naked or sexual picture of you without your consent they're breaking the law. It's not always possible to get these images taken down but there's a special Revenge Pornography Helpline for people who are over 18 that can help.

Getting the message across

Imagine taking a squeezable tube of paint: the paint represents everything we say digital. Squeeze the paint out and see how difficult it is to get it back into the tube. This is exactly what it is like when we say something digital – we can never take it back.

Staff

This is a really difficult issue for staff to have to deal with. If you believe that pupils have been sexting illegally then the situation needs to be dealt with as seriously as you would investigate cases of bullying. First try and establish facts.

- Who sent what to who?
- How old are they?
- What were the images of?

You do not want to be in a position where you feel you have to look at the images yourself. Avoid that at all costs.

Staff need to feel confident talking to pupils and talking to parents about incidents of sexting, and be clear on the law.

It's very unusual for the police to prosecute in cases of sexting in schools, but it can happen and everyone must be aware of that.

LAST UPDATED: 05 DEC 2016

UKCCIS

UK COUNCIL FOR CHILD INTERNET SAFETY

Sexting: how to respond to an incident. An overview for all teaching and non-teaching staff in schools and colleges

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.
All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.
The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), **Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People,** and should **not** refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention - r**eport it to your Designated Safeguarding Lead (DSL) immediately.**

- Never view, download or share the imagery yourself, or ask a child to share or download – this is illegal.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

Your school's safeguarding policies should outline codes of practice to be followed.

For further information download the full guidance *Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016)* at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'. All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line

ANNEX D: CONSENT FORM FOR PHOTOGRAPHS

KING EDWARD VI ACADEMY TRUST BIRMINGHAM PHOTOGRAPHY POLICY

The Schools of King Edward VI in Birmingham (the 'Charity') and King Edward VI Academy Trust Birmingham (the 'Academy Trust') (collectively the 'Foundation') are obliged to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (collectively the 'Data Protection Regulation') when it takes or publishes photographs and videos of its pupils. The Foundation will always try to act in the best interest of the pupils and, as far as it legally can, it will take parental preferences into account.

The Data Protection Regulation gives children rights over their own data when they are considered to have adequate capacity to understand. Most children will reach this level of understanding at around age 12. For this reason, for most pupils in a secondary school, it will normally be up to the individual child to decide whether or not to be photographed/videoed. Where the school considers that the child does not have the capacity to make such a decision the school will act as it considers to be in the best interests of the child and in doing so will take account of any stated parental preference.

If you wish to express a preference for the school to avoid taking or publishing photographs or videos of your child in certain circumstances, then please indicate your preferences using the attached form. If no preferences are expressed, then we will act in accordance with the principles expressed in this policy.

Ordinarily the following rules will apply to photographs/videos in the Foundation:

Photographs for Internal Use

- The Foundation will take photographs/videos for its own use. Usually these will be unnamed photographs and will generally be for internal school use but may also include photographs for publication, such as photos for the prospectus, on the Foundation and school websites/social media or to show as slides at an event for parents. Unnamed photographs may also be used on display boards which can be seen by visitors to the school.
- When the photograph is taken, the pupils will be informed that a photograph is being taken and told what it is for so that they can object if they wish.
- If the school wants to use named photographs, then it will obtain specific consent first. For most pupils this will be pupil consent as explained above but parental wishes will be taken into account.

Media Use

- The school will give proper consideration to the interests of its pupils when deciding whether to allow external organisations to take photographs or to film.
- When the Media are allowed to be present in school or at school events, this will be on the condition that they observe this policy.
- Where the media are allowed to be present at a particular event the school will make sure that pupils and their parents or carers are informed of the media presence. If no objection is received, then the school will assume that unnamed photographs may be published.
- If the Media entity wants to publish named photographs, then they must obtain specific consent from those pupils with capacity to consent or the parents of those without capacity. The school will require the media entity to check with the school before publication so that the school can check that any objections have been taken into account.

Family Photographs at School Events

• It shall be at the discretion of the school whether photographs may be taken at a school event.

• Family and friends taking photographs for the family album will not be covered by Data Protection legislation.

• Where the school decides to allow such photography, the family and friends will be asked not to publish any photographs showing children other than their own on the internet.

EXPRESSION OF PARENTAL PREFERENCES

Name of Child: ____

School: ____

Unnamed photographs

- Unnamed photographs/videos of my child can be used in school.
- Unnamed photographs/videos of my child can be used for wider publication such as:
  - School prospectus and similar information
  - Foundation and School websites
  - Social Media
  - Display boards
  - Unnamed photographs/videos of my child can appear in any external publication.

YES / NO

Named photographs

- Named photographs/videos of my child can be used in school.
- Named photographs/videos of my child can be used in any school publication.
- Named photographs/videos of my child can be used on the Foundation and School websites, as well as social media.
- Named photographs/videos of my child can appear in any external non-school publication.

YES / NO

I understand that the school will try to take my preferences into account but that the school and the Foundation must comply with the Data Protection Regulations which will give my child rights in his/her own data when he/she has adequate capacity and understanding to make decisions about the publication of his/her photographs/videos for him/herself.

Signed: ....

PRINT NAME: ....

Relationship to child: ....

ANNEX E:

GUIDANCE PAPER

ASCL Association of School and College Leaders

SOCIAL NETWORKING, SOCIAL MEDIA AND EMAIL: PROTECTING YOUR PROFESSIONAL REPUTATION: June 2017

GUIDANCE AT A GLANCE

This guidance paper is relevant to all staff in all schools and colleges. It offers information and guidance when considering the safeguarding of staff in their use of social networking sites (SNS), such as Facebook, Twitter and Instagram, both at school and personally. The open nature of the internet and social networking means that everyone – including senior leaders – should take active steps to protect themselves and their school or college by taking simple precautions.

Your professional reputation is part of your current and future career, therefore managing your digital reputation is essential.

Anything you post digital or send by email is potentially public and permanent, even if you subsequently delete posts and emails and if you use privacy settings.

ASCL strongly advises that you do not accept friend or follow requests on your personal accounts from pupils, past or present, or from parents at your school or college. By accepting such requests you could make yourself vulnerable by sharing personal information or by having access to personal information about pupils. This could leave you open to allegations of inappropriate conduct, as well as exposure to unwanted contact.

This guidance covers the following areas:
Section 1 Protecting your professional reputation
Section 2 Privacy settings and password security
Section 3 Managing content and reporting abuse
Section 4 Further information

1 PROTECTING YOUR PROFESSIONAL REPUTATION

Your professional reputation is part of your current and future career therefore managing your digital reputation is essential.

Anything you post digital or send by email is potentially public and permanent, even if you subsequently delete posts and emails and if you use privacy settings.

On SNS, friends can re-post or comment on your posts which means others to whom you have not given access may view your comments.

Think carefully before posting information about your school, college, staff, pupils or parents – even if your account is private. Comments could be taken out of context and be damaging. The language you use is important, as abrupt or inappropriate posts may lead to complaints.

Think about how you present yourself when you post images, when joining a group or 'liking' pages; these choices say something about you. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post or image in the public domain will lower the reputation of the school or college and that could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer. In addition, potential employers may also look digital and you will want to consider whether your choices show you in the best light when applying for a job.

SNS are utilised by some schools and educators as a means of connecting with parents, governors and students, however, this is done via organisational or professional pages and accounts. Prior approval is also obtained from the senior leadership team, and it should be borne in mind that 13 is the minimum age requirement of most SNS.

2 PRIVACY SETTINGS AND PASSWORD SECURITY

When using social networking websites it is important that you are in control of who can see your account details and content, including photos, albums, posts, status updates and any personal information. Accounts for Twitter, Facebook and Instagram can be set to private by following these steps:

Twitter

1. click 'profile and settings' cog icon at the top right of the Twitter homepage
2. select 'settings'
3. select 'security and privacy' from the left-hand menu
4. tick 'protect my tweets' check box
5. click 'save changes'

By selecting the 'protect my tweets' option you will be able to either accept or decline requests to follow you.

Facebook

Choosing the 'friends only' setting for every option enables a good degree of privacy. Amend your Facebook privacy settings as follows:

1. click on 'privacy' padlock icon, at the top right of your wall
2. review 'who can see my stuff', 'who can contact me' and 'who can look me up'
3. select 'edit' on the drop-down menu

Instagram

By default, anyone can view your profile and posts on Instagram. You can make your posts private so that only followers you approve can see them. If your posts are set to private, only your approved followers will see them in the Photos tab of Search and Explore or on hashtag or location pages. Posts can't be set to private from a desktop computer.

To set your posts to private from the Instagram app:

iPhone or Windows Phone

1. Go to your profile by tapping 👤
2. Tap ⚙
3. Turn on the Private Account setting

Android

1. Go to your profile by tapping 👤
2. Tap ⋮
3. Turn on the Private Account setting

Updates to your privacy settings are automatically stored and do not need to be saved manually. Furthermore, you can customise each option and limit the information certain people can see. It is always useful to use the 'view as' option, to check how your profile appears to others and that the information you want to remain private or for 'friends only' is not visible to everyone. If you are not entirely sure about how to use all the settings, treat all of the information that you post as being available to everyone and act accordingly.

Friend or foe?

It is a good idea to remove any friends, or customise the privacy settings for current friends, if access to your personal activity could compromise your position. It is important, regardless of which setting you use, that you assume that every post you make could be made public, because 'friends' settings do not guarantee privacy.

Be careful about comments you post on your friends' walls; if their profile is not set to private, your posts will be visible to everyone. Sharing content with others means that it is out of your control.

It is important, regardless of which setting you use, to assume that every post you make could be made public, as friends' settings do not guarantee privacy.

Geo-location services

There are clear implications about making sensitive information public. If using this feature on SNS, consider making your location visible only to your friends. It is also possible to disable the feature by which someone else can 'check you into' a location within your privacy settings, enabling you to control what information is shared.

Password and security

- Always use a strong password that contains a combination of upper and lowercase letters and numbers and ensure that it is at least six characters long.
- Do not select the 'remember this password' option when logging on to a shared computer or device as others may later be able to access it.
- Log out after you have finished digital. Not logging out means the next user can access your social networking account.
- Always set a PIN or passcode on your mobile phone or tablet so access to your account is still protected if you lose it.
- Keep anti-virus software up-to-date

Robust security settings could prevent hacking. Further, if an employee has kept up a reasonable degree of security and if the hacker clearly had to get through serious barriers then the exposure of material could be excusable, there was a reasonable expectation of privacy. However, if confidential information that should have remained within the organisation has been revealed, the fact that the leak has been exposed is irrelevant.

3 MANAGING CONTENT AND REPORTING ABUSE

Search your name regularly digital to monitor any content about yourself. This enables you to see what others see and provides an opportunity for you to delete anything that may compromise your reputation. Be aware of what monitoring, if any, is carried out by the school or college.

Other people could post images on their profile in which you are named, so think about any photos you appear in. On Facebook you can 'untag' yourself from a photo. If you do find inappropriate references to you or images of you posted by a friend digital, you should contact them and ask for that content be removed. Alternatively, report directly to Facebook to request its removal, although it will be Facebook's judgement as to whether it remains digital.

In 2014 a European ruling against Google stated that the search giant must delete "inadequate, irrelevant or no longer relevant data" from its search results when requested. In theory, Google must remove links to personal information that is not relevant or in the public interest. However, the reality is that requests will still have to go through the courts resulting in a complicated battle. The information will still be available on the web, it won't be visible through a Google search.

Using email

All emails sent from a school or college account should be regarded as public, especially as a 'data subject access' request could be made under the Data Protection Act. Emails should always be in professional language and appropriate to being an employee. It should also be noted that where a private email account is used for issues associated with work, it has in some cases been deemed as a work account and therefore also subject to the rules of professional language and conduct.

In short, do not send a private email that you would not be happy for your employer or a colleague to read.

Digital harassment

Sometimes remarks aimed at an individual or the school or college go beyond inappropriate and become offensive and abusive. The best option is not to draw attention to these or escalate the issue; when ignored, the offended party may give up and the remarks end up being seen by only a handful of disgruntled individuals. However, if this continues it can become harassment.

There is a duty of care on the part of your employer to protect you from harassment. If they fail in this duty and you suffer harm they could be legally liable. Your first course of action is to contact the service provider to delete the offending remarks or close down the website. If this is not successful, ASCL considers it appropriate for the employer, rather than you, to take legal action to tackle the issue (or make use of the employer's legal advisers, for example the LA or retained lawyers), both because the employer should be protecting its employees from harassment and a slur on an employee is also a slur on the employer.

If the comments are offensive and sufficiently frequent they can be deemed as harassment in the criminal sense and should be reported to the police.

Unfortunately, it is difficult to make a legal case for defamation. For a statement to be defamatory it must tend to lower the claimant in the estimation of right-thinking members of society generally. A statement that amounts to an insult or is vulgar abuse is not defamatory. This is because the words do not convey a defamatory meaning to those who heard them (simple abuse is unlikely to cause real damage to a reputation).

Before you decide how you wish to proceed, consider that minimising any publicity will be a factor in your decision-making.

School and college policies

Schools and colleges should have a detailed policy about the use of information communication technology, including social media. ASCL strongly advises that this policy states staff should not make contact with students through staff personal emails, by text on their personal phones or on social media sites. ASCL is seeing an increase in cases where behaviour of staff is either taken out of context or could be construed as questionable. Having a blanket ban on personal and private communication protects both staff and pupils.

Your school or college policy should also include specific guidance on the use of SNS. If the school or college encourages the positive use of SNS as part of the educational process then it should provide clear guidance on what is considered appropriate contact with students. Again, having a clear policy in place will help staff and pupils to keep within reasonable boundaries.

4 FURTHER INFORMATION

Support from ASCL

If you are facing disciplinary action because of something you have posted digital or find yourself the victim of abusive digital posts and cannot resolve the matter directly with the digital service provider, please contact ASCL Hotline on 0116 2991122 or email hotline@ascl.org.uk

Guidance papers

Guidance paper: *An exploratory evaluation framework – safety and safeguarding, equalities, British values, the curriculum and governance*
Guidance paper: *Statutory duties related to safety and safeguarding, equalities, British values, the curriculum and governance*