



E-Safety Policy

Policy Title:	E-Safety Policy
Last Review:	September 2026
Next Review:	September 2027
Responsibility:	Designated Safeguarding Lead, Headmaster
Other relevant policies:	Complaints Policy Computing and ICT Policy Data Protection Policy and Privacy Notices Off-site Activities and Educational Visits Policy Prevent Policy PSHE Policy Pupil Behaviour Policy Safeguarding and Child Protection Policy Staff Code of Conduct Staff Handbook Taking, Storing and Using Images of Children Policy

1. Aims and Objectives

It is the duty of West House School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Staff Handbook, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

At West House School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

West House School ensures that its filtering and monitoring systems meet the Department for Education's statutory Filtering and Monitoring Standards (2023). This includes robust technical filtering, active monitoring, clear governance oversight, defined incident-response procedures, and regular review of system effectiveness. The DSL and IT Consultants work together to ensure that filtering and monitoring remain appropriate, proportionate and safe for all users.

2. Scope

This policy applies to all members of the West House school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff, peripatetic staff, governors, and volunteers;
- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

Both this policy, and the Bringing Your Own Device to School Policy, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Pupil Behaviour Policy and Safeguarding and Child Protection Policy as is appropriate in the circumstances.

The school conducts regular online safety risk assessments to identify emerging risks, evaluate the effectiveness of current controls, and ensure compliance with statutory safeguarding duties. These assessments inform updates to filtering, monitoring, staff training, curriculum content and parental guidance.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the DSL are adequately trained about online safety;

- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Headmaster and the Senior Leadership Team

The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

In line with the Anti-Bullying Policy the Headmaster will personally address any allegations of online bullying (cyber-bullying).

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at West House School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Senior Leadership Team (SLT) and IT Consultant. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work to ensure that the school's requirements for filtering and monitoring are met and enforced. With effect from September 2024, the school has implemented a new Filtering and Monitoring system "Smoothwall" which provides the DSL with full current checks of the system for all staff, pupils and visitors accessing our network and wireless internet. Any inappropriate usage is reported immediately to the DSL.

The DSL will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The DSL will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's Smoothwall filtering and monitoring system to the SLT.

3.4. IT Consultants

The school's IT Consultants (Harborne Computers) have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They maintain content filters in connection with the DSL and Smoothwall.

3.5. Head of ICT

The Head of ICT will ensure there is a rigorous curriculum for Computing in which pupils across the school have specific lessons to learn how to be safe online.

Takes opportunities such as 'Safer Internet Day' to broadcast positive messages to the school community about esafety.

3.6. Teaching and support staff

All staff are required to read the Staff Handbook which includes the use of IT and Devices, and sign via Edupay to agree to adhere to correct use of the school's systems. As with all issues of safety at this school, staff are encouraged to

create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

In lessons, staff ensure:

- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils have a good understanding of online safe research skills
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

In accordance with KCSIE 2025, all staff receive annual safeguarding training that includes online safety, filtering and monitoring, cyber-security awareness, and digital safeguarding responsibilities. Staff also receive regular updates throughout the year. The DSL receives advanced online safety training, and governors receive training to ensure effective oversight of filtering, monitoring and digital safeguarding.

3.7. Pupils

Pupils are responsible for using the school IT systems in accordance with relevant policies and advice.

They should have a good understanding of safe research skills and adopting a good E-Safety practice when using digital technologies in and out of school.

Need to understand the importance of reporting abuse, misuse of access to inappropriate materials to the teacher or DSL.

3.8. Parents and carers

West House School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

West House has an Online Safety Hub for parents to access providing detailed information and Podcasts.

4. Filtering and Monitoring

In general:

West House School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to **all users**, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The school uses Smoothwall as its filtering and monitoring system and by using an external system, the provider is responsible for ensuring the effective operation. This filtering can support users engaged in home learning to use devices safely outside the formal filtering that exists within the school premises.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content and adult content. If there is a good educational

reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy and/or Privacy Notice, any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the DSL if they are teaching material which might generate unusual internet traffic activity.

The Servers, wireless systems and cabling is securely located and physical access restricted.

The Administrator passwords for the school ICT system, used by the Network Manager is also available to the Headmaster and kept in a secure place.

Harborne Computers is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Staff:

If any member of staff has any concern about the effectiveness of the Smoothwall filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the IT Consultant if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the DLS for assistance.

5. Education and training

5.1. Staff and Volunteers: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT curriculum. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, in assemblies, as well as informally when opportunities arise.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

We recognise that educating our children to make wise choices about how they behave online is the most important thing we can do. Whilst in school they have a protected and well-filtered environment, surrounded by positive role models and we must inculcate the children with the skills, confidence and attitudes to make good choices as they progress through education and into adult life. Therefore, the robust and rigorous curriculum with specific e-safety lessons and e safety referred throughout is the core of our strategy.

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety Curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety Curriculum is provided as part of ICT and PSHE lesson, along with input from Life Education Centres who present a 'Cyberwise' programme to all pupils in Years 3 – 6.
- Key E-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Senior pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff are required to act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Online safety education follows a sequenced and progressive model from Nursery to Year 6. Learning outcomes are mapped to the UKCIS Online Safety Framework and revisited with increasing depth as pupils mature. Pupils are taught age-appropriate content relating to digital resilience, critical thinking, online relationships, privacy, misinformation, cyberbullying, and safe use of emerging technologies.

5.3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through

- The 'E-Safety Advice for Parents of Boys in Years 5 and 6' information sheet (Appendix A)
- Letters, newsletters, web site
- Parents sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

6. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Staff Handbook for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at West House School are permitted to bring in personal devices for their own use. Staff are not allowed to have their personal devices switched on during the working day. They may use such devices in the main school staffroom during break-times and lunchtimes.

Pupils

School mobile technologies made available for pupil use by the school including laptops, Chrome Books, cameras, etc. are stored in classrooms. Access is available during lessons via teachers.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

Remote Learning and Online Teaching

Where remote learning or online teaching takes place, staff and pupils must follow the school's safeguarding expectations. This includes using school-approved platforms, ensuring appropriate supervision, maintaining professional conduct, following privacy requirements, and adhering to guidance on recording, screen sharing and digital communication. Remote learning must always comply with the Safeguarding and Child Protection Policy.

7. Online Communications

Staff

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / recent alumni or parents of recent West House Old Boys

using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. Under no circumstances may staff contact a pupil or parent / carer and recent West House Old Boys using a personal telephone number, email address, or other messaging system nor should pupils, parents be added as social network 'friends' or similar.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Consultant.

Pupils

All pupils in Year 3 and above are issued with their own personal school email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system.

8. Use of social media

Staff

Staff must not access social networking sites, personal email from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room.

When accessed from staff members' own devices, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct and Staff Handbook.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring West House School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - using social media to bully another individual; or
 - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

9. Data protection

Please refer to the Data Protection policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to their school laptop / PC or to the school's One Drive Account.

Staff devices are encrypted if any data or passwords are stored on them.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Consultant.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Consultant.

10. Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

11. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's Taking, Storing and Using Images of Children policy.

Artificial Intelligence

West House School does not permit the use of generative AI tools such as ChatGPT on school devices / systems. In particular, personal or confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature.

Artificial Intelligence and Emerging Technologies

The school recognises the safeguarding, data protection and ethical risks associated with generative AI and emerging technologies. Staff and pupils must not input any school-related, personal or sensitive information into AI tools. The DSL will assess risks associated with new technologies and ensure that any permitted use complies with safeguarding, data protection and cyber-security requirements.

12. Misuse

West House School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

Cybersecurity Responsibilities

In line with National Cyber Security Centre (NCSC) guidance, the school maintains robust cyber-security practices including secure device management, regular patching and updates, phishing awareness, incident-response procedures, and secure handling of data. Staff must report suspected cyber-security incidents immediately to the DSL and IT Consultant.

13. Complaints

As with all issues of safety at West House School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Bursar in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's DSL in accordance with the school's Safeguarding and Child Protection Policy.



Appendix A

E-safety Advice for Parents of Boys in Years 5 and 6

E-safety relates to phones, tablets, computers, apps, social media, etc. Issues surrounding e-safety are discussed with boys in Years 5 and 6 at the start of the academic year and addressed through assemblies and PSHE lessons. In so doing, we emphasise the many benefits of the technology to underline the fact that we do want boys to use it – but kindly, and with their eyes open to the potential pitfalls. It would be naïve of all of us to assume that your son will not be exposed to at least some of these pitfalls in the coming months and years.

Social Media

We strongly suggest that you look at your son's phone, tablet and computer with him every few weeks. What apps is he using? What online friends does he have? How is he communicating with them? It is unwise in the extreme for boys of this age to have online friends whom they do not know in real life. You may consider adopting a 'no screen upstairs' rule so that your son learns that what he does online is in the public domain.

Are you content with your son's choice of games and social media, given the age recommendation for each app? Make a point of reviewing, with your son, the safety and security settings on the main apps or social media that he uses. It is possible for children to use social media safely with the correct adult supervision but the rules of such sites are clear: they are all 13+. Should any inappropriate use of social media come to the school's attention, we will contact the provider and have the account deleted.

Photos and Videos

The camera facility on their phone or watch is a particular draw for children. However, young people do make some quite serious mistakes, so we say this to boys:

- Only take photos or videos with the permission of the people you are photographing.
- Don't upload photos or videos to online apps / social media – that is so fraught with trouble that at this age it is simply not appropriate.

'Sexting'

Boys must never take photos or videos of people (or themselves) when they are half dressed or naked. Sending such photos as well as texts of an explicit or suggestive nature is called 'sexting' and seems to be a real issue as children approach puberty. Whilst this behaviour would appear shocking to many adults, it is surprisingly common amongst young people and our older boys are approaching an age at which they may be tempted to engage in such activities.

Pupils do need to be aware that sending indecent images of a child (including an indecent 'selfie') is illegal and thus could have serious consequences. Due to the illegal nature of this issue, the school is required to report instances of sexting to the Birmingham Safeguarding Children Board, and to take advice on whether police need to be involved.

Cyber-bullying

We tell boys that what they do and say online must, crucially, be kind, and that one good way to test the appropriateness of what they are doing is whether they would be happy for their parents or grandparents to see it.

Examples of troublesome behaviour would be any unkind, racist or homophobic remarks, or targeting someone, or spreading gossip, or uploading photos/videos that could cause offence or upset. The school will investigate such behaviour, regardless of whether it happens on or off site. Often boys are not fully aware of the effects and

consequences of their actions, and when we explain these, problem behaviour can often be resolved relatively easily. Sanctions may be imposed in accordance with the Anti-Bullying Policy.

Stranger Danger

Sadly, we know that paedophiles use the internet and apps, and boys are targets as well as girls. Children are inquisitive, biddable and trusting, and thus vulnerable. We suggest to boys that:

- They do not join any chat rooms or groups on apps or social media. However, it is possible that they will join groups with their friends.
- They need to be aware that it is fairly easy for others who they don't actually know to get into online groups.
- It is important not to reveal their address, mobile number or planned locations via ANY app or social media. They should pass that kind of information in via e-mail, text, phone calls or face-to-face and only to trusted friends.
- If something goes wrong, they should tell a trusted adult.

Use of Mobile Technology at School

Boys are not allowed to bring their own mobile devices, including phones, to school unless specifically given permission to do so. Specific guidance about the use of mobile technology will be given in relation to residential and non-residential trips and visits. It is an expectation of the school that such guidance is followed.

Sensible Limits

Many boys will play games obsessively if allowed to do so. It is important that parents monitor how much time their sons are spending watching television, or playing on tablets, computers and phones. The boys should not have such distractions at bedtime and while they are doing their homework. If they get the balance right it is, of course, perfectly reasonable for them to have a certain amount of 'guilt-free time' when they can engage in the use of such technology.

Prank Calls

Boys should be cautious about giving their telephone number out. When they first get a phone, the temptation is to share numbers and this can precipitate episodes of prank calls. The boys are reminded that such calls cause more annoyance and offence than they realise and that they must not allow this to happen.

Popular Apps and their Dangers

There are a number of extremely popular apps which, in spite of recommended age restrictions, some of our boys use. One such example is 'Clash of Clans'. This is a game, but with a chat facility in the background, meaning that children can and will converse with other users of the app. Many other users are not children and it is essential that the boys are aware of this and act with extreme caution.

Some pupils are already using Snapchat, Instagram and WhatsApp. The necessity to be cautious is equally applicable to these cross-platform messaging apps.

If a Problem Arises

Everyone makes mistakes. We tell boys that if something has gone wrong – either something they have done, or that someone else has done, they should tell a trusted adult. Such adults include parents, form teachers, a member of the Senior Leadership Team, or Mr Regall who is the Head of STEM. Children are likely to feel embarrassed, or feel that nothing can be done – when in fact there are helpful steps that we can take.

The Future

The world of technology develops rapidly, and so do pupils as they progress towards their secondary school years. For these reasons, the school holds e-safety lessons with all forms every year to address the latest issues as they arise.

Contacting us

If you would like to discuss any of these issues, please get in touch. You could speak to your son's Form Tutor, Mr Regall or a member of the Senior Leadership Team.