ICT and Internet Acceptable Use Policy

Aims

This is the acceptable use of ICT policy for pupils at Kirkstone House school.

The aims of the policy are as follows:

to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

to safeguard and promote the welfare of pupils, in particular by anticipating and preventing risks arising from:

- exposure to potentially illegal, harmful or inappropriate content (such as pornographic, racist, extremist or offensive materials);
- the sharing of personal data, including images;
- inappropriate online contact or conduct, including sexual harassment;
- cyberbullying and other forms of abuse; and
- online challenges and online hoaxes.

to minimise the risk of harm to the assets and reputation of the school;

to help pupils take responsibility for their own safe use of technology;

to ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology;

to prevent the unnecessary criminalisation of pupils; and

to help to promote a whole school culture of openness, safety, equality and protection.

This policy forms part of the School's whole approach to promoting child safeguarding and well-being which involves everyone in the School and seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

Scope and application

This policy applies to pupils using or accessing the school's technology whether on or off School premises, or using their own or others' technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation and orderly running of the School are put at risk.

Parents are encouraged to read this policy with their child. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

Regulatory framework

This policy has been prepared to meet the School's responsibilities under:

- education (Independent School Standards) Regulations 2014;

- Education and Skills Act 2008;
- Childcare act 2006;
- Data Protection Act 2018 and UK General data Regulation (UK GDPR); and
- Equality Act 2010.

This policy has regard to the following guidance and advice;

- Keeping Children safe in education (DfE, September 2025);
- Preventing and tackling bullying (DfE, July 2017);
- Sharing nudes and semi-nudes: advice for educational settings working with children and young people (Department for Digital, Culture, media and Sport (DfDCMS) and UK Council for Internet Safety (UKCIS) March 2024);
- Technical guidance for schools in England (Equality and Human Rights Commission, July, 2024);
- Relationships education, relationships and sex education and health education guidance (DfE, September 2021);
- How can we stop prejudice-based bullying in schools? (Equality and Human Rights Commission);
- Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);
- Searching, screening and confiscation: advice for schools (DfE, September 2022);
- Mobile phones in schools (DfE, February 2024); and
- Behaviour in schools: advice for Headteachers and school staff 2022 (DfE, February 2024).

The following School policies, procedures and resource materials are relevant to this policy:

Behaviour and Discipline Policy;

Anti-bullying pupils;

Online Safety policy;

Permanent Exclusion and removal Review Procedure;

Safeguarding Policy and Child Protection Policy procedures;

Relationships Education and relationships and sex education;

Risk Assessment for Pupil welfare;

Inclusion and Diversity Policy and

Preventing Extremism and radicalisation policy.

Publication and availability

This policy is available in hard copy on request.

A copy of the policy is available for inspection from the school office during the school day.

This policy can be made available in large print or another accessible format if required.

Definitions

The School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology). This policy relates to all technology, computing and communication devices, network hardware and software and services and applications associated with them including:

- the internet;
- email and school messaging platforms;
- generative AI technology / tools;
- electronic communications;
- mobile phones and smart technology;
- desktops, laptops, netbooks, tablets;
- personal music players;
- devices for recording and / or storing still or moving images;
- social networking, micro blogging and other interactive websites;
- instant messaging, video hosting sites (such as youTube);
- gaming sites;
- virtual learning environments;
- SMART boards, display screens;
- Other photographic or electronic equipment;
- Devices which allow sharing services offline.

Responsibility and allocation of tasks

Task	Allocated to	Review
Keeping the policy up to date and compliant with the law and best practice	On-line safety lead	As required and at least annually
Monitoring the use of technology across the School and recording any concerns / incidents on C-POMS	On-line safety lead	As required and monitoring at least termly.
Ensuring the policy remains up to date with technological change	Office Friends / Headteacher	As required and at least termly.
On-line safety	DSL	As required and at least annually
Formal Annual review	Proprietor and safeguarding Advisor	Annually

Safe use of technology

We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is a crucial factor for further education and careers.

The school will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of

our systems. The safe use of technology is integral to the School's curriculum. Staff are aware that technology can be a significant component in many safeguarding and wellbeing issues and pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Pupils may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk

http://www.childnet.com/resources/smartie-the-penguin#https://www.saferinternet.org.uk/advice-centre/young-people

http://www.childline.org.uk/Pages/Home.aspx

https://www.ceop.police.uk/Safety-centre/How-can-CEOP-help-me-YP

Internet

The School provides internet and receive guidance on its use. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff. Pupils are given individual usernames and passwords and these details must not be disclosed to anyone else.

No laptop or other electronic mobile device may be connected to the School network without the consent of the Head of ICT.

For the protection of all pupils, their use of e-mail and internet will be monitored by the School. Pupils should remember that even when an e-mail that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers are always private.

School rules

Pupils must comply with the following rules and principles:

- Access and security (Appendix 1)
- Communicating on or off-line using devices (Appendix 2)
- Use of mobile electronic devices and smart technology (Appendix 3)
- Photographs and images (including consensual and non-consensual sharing of nude and semi-nude videos (Appendix 4)
- Online sexual harassment (Appendix 5)
- Harmful online challenges and hoaxes (Appendix 6)

The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely. These principles and rules apply to all use of technology in school and at home whether during or outside School.

Procedures

The way in which pupils relate to each other online can have significant impact on the School's culture. Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Even though online space differs in many ways, the same standards

of behaviour are expected online as apply offline. Use of technology should always be safe, responsible and respectful to others and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher about it immediately.

Any misuse of technology by pupils will be dealt with under the school's behaviour and Discipline Policy. Incidents involving misuse of technology which are considered to be of a safeguarding nature will be dealt with in accordance with the school's safeguarding and Child Protection Policy and procedures, rather than the school's Behaviour and Discipline Policy.

Pupils must not use their own technology or the School's technology to bully others. Bullying incidents involving the use of technology, including cyberbullying, prejudice-based bullying and discriminatory bullying will be dealt with under the School's Anti-bullying Policy. If a pupil thinks they might have been bullied or that another person is being bullied, they should talk to a teacher or trusted adult as soon as possible.

The School has adopted a zero tolerance to sexual violence and sexual harassment; it is never acceptable and will not be tolerated. Incidents of sexual violence or sexual harassment will not be dismissed as merely 'banter' or 'just having a laugh' or 'boys being boys' as this can lead to the creation of a culture of unacceptable behaviours and an unsafe environment for children and in the worst- case scenarios, a culture that normalises abuse.

Sexual harassment, in the context of this policy, means 'unwanted conduct of a sexual nature' and the School recognises that this can be online or offline. Pupils must not therefore use their own technology or the School's technology to sexually harass others at any time whether during or outside School. Incidents of sexual harassment involving the use of technology will be dealt with under the School's behaviour and Discipline and Safeguarding Policies. If a pupil thinks that they might have been sexually harassed or that another person is being sexually harassed, they should talk to a teacher or a trusted member of staff as soon as possible.

The school recognises that children's sexual behaviour exists on a wide continuum ranging from normal and developmentally expected to inappropriate, problematic, abusive and violent. Problematic, abusive and violent sexual behaviour is developmentally inappropriate and may cause developmental damage. Such behaviour can be classed under the umbrella term 'harmful sexual behaviour'. The School is aware that this can occur online and or offline. Face to face and can occur simultaneously between the two.

Any reports of sexual violence or sexual harassment will be taken extremely seriously by the School and those who have been victim to such abuse will be reassured, supported and kept safe throughout. No pupil should ever be made to feel that they have created a problem or feel ashamed for reporting their concern. Pupils should be aware that teachers may not be able to provide a reassurance of confidentiality in relation to their concern as information may need to be shared to consider next steps. (See appendix 5 for further information).

The designated safeguarding Lead takes responsibility with in the School for safeguarding and child protection. The Head of Pastoral care takes a joint responsibility for online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures. If a pupil is worried about something they have seen on the internet or on any electronic device, including another person's electronic device, they must tell a member of staff about it as soon as possible.

The School is also aware of the risks of radicalisation and understands that this can occur through many different methods (including social media or the internet). In a case where the pupil is considered to be vulnerable to radicalisation, they may be referred to the Chanel programme. Chanel focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

Cybercrime:

Cybercrime is criminal activity committed using computers and / or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that happen off line but are enabled at scale and at speed online) or 'cyber-dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

- Unauthorised access to computers (illegal hacking) for example, accessing a school's computer network to look for test papers or change grades awarded;
- Denial of service (DoS or DDoS) attacks or 'booting' which are attempts to make a computer, network or web site unavailable by overwhelming it with internet traffic from multiple sources, and
- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offences, including those above.

The School is aware that pupils with particular skill an interest in computing and technology may inadvertently or deliberately stray into cyber dependent crime.

Any concerns about a pupil in this area will be referred to the DSL immediately. The DSL will then consider referring to the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the national crime Agency working with regional and local policing.

All serious incidents involving technology must also be reported to the Headteacher and the head of Pastoral care who is the online safety lead.

Generative Artificial Intelligence:

When using any generative AI technologies pupils are expected to consider the following;

- AI and human intelligence are not the same. AI tools do not understand what they produce or the impact the generated content may have;
- Sometimes AI tools will generate answers that sound plausible but they may not be correct;
- Content produced may perpetuate harmful biases and stereotypes and may not be age-appropriate;
- Over-reliance on these tools will reduce opportunities to improve research skills, writing and critical thinking;
- AI tools store and learn information submitted to them so personal data should never be entered;
- If teachers indicate that pupils are permitted to use generative AI technologies in their work, pupils must observe all related instructions and guidance; and

- Submitting work produced in whole or part by AI with out proper referencing or acknowledging use of AI may be considered cheating / plagiarism and inappropriate use of AI.

Any misuse or inappropriate use of AI technologies by pupils will be addressed in accordance with the school's behaviour and Discipline Policy and disciplinary procedures.

The School may implement measures to ensure the safe and appropriate use of AI technologies within its network. These measures may include monitoring AI activities, restricting access to certain AI systems or providing guidelines and restrictions on the use of specific AI applications.

Sanctions

Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Headteacher will apply any sanction which is appropriate and proportionate set out in the School's behaviour and Discipline Policy, including in the most serious cases, permanent exclusion. Other sanctions might include: increased monitoring procedures; withdrawal of the right to access the School's internet and email / electronic communication facilities and fixed term suspension. Any action taken will depend on the seriousness of the offence.

Unacceptable use of technology could lead to the confiscation of the device or deletion of material in accordance with the procedures in this policy and the section Searching and Confiscation in the School's Behaviour Policy.

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains pornographic image of a child or an extreme pornographic image, the device will be given to the police.

The school reserves the right to charge a pupil or their parents for any costs incurred to the School as a breach of this policy.

Training

The School ensures that:

regular training is given to staff so that they understand what is expected of them in relation to this policy;

that they have the skills and knowledge to carry out their roles; and

that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

Staff development is regularly updated and on-going staff development training includes, but is not limited to:

Training on specific safeguarding issues such as sharing nudes and semi-nudes, cyber-bullying, radicalisation, and dealing with harmful online challenges and hoaxes.

The level and frequency of training depends on the role of the individual member of staff.

The school maintains records of all staff training.

Risk Assessment

The School recognises that technology and the risks and harm associated with it, evolve and change rapidly. The School will carry out regular, and at least annual reviews of its approach to online safety supported by risk assessment which consider and reflect the risks faced by its pupils.

Where a concern about a pupil's welfare is identified, the risks to that pupils' welfare will be assessed and appropriate action will be taken to reduce the risks identified.

The format of the risk assessment may vary and may be included as part fo the School's overall response to a welfare issue, including the use of individual pupil welfare plans, EHCPs as appropriate. Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

The Headteacher has overall responsibility for ensuring that matters which affect pupil welfare in School are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated. She works closely with the DSL, Head of Pastoral care / Online Safety Lead, teacher of ICT and Office Friends, an external provider.

Record Keeping

All records created in accordance with this policy may contain personal data. The School's use of personal data will be in accordance with data protection law.

Date of adoption of the policy:	September 2025
Date for next review:	September 2026 or before if required.
Author: Headteacher	Mrs C L Jones
Authorised by:	Mr E G Wyman Proprietor
Circulation:	Staff, Parents and Senior School Pupils.

Appendix 1 Security

Access to the internet from the School's computers and network must be for educational purposes only.

Pupils must not knowingly obtain or attempt to obtain unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

No laptop or other mobile electronic device may be connected to the School network without the consent of the Headteacher.

Passwords protect the School's network and computer system. Pupils understand that they must not share passwords or tell others what their password is. If pupils believe that someone else knows their password, they understand that they must change it.

Pupils understand that they must not attempt to gain unauthorised access to anyone else's computer or user account or to confidential information to which they are unauthorised to access. If there is a problem with passwords, they need to report this to the ICT teacher.

Pupils must not attempt to access or share information about others without the permission of the Teacher of ICT. To do so may breach data protection legislation and laws relating to confidentiality.

The School has security hardware and software meeting digital and technology standards in place to ensure the security and safety of the School's networks. Pupils must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the hardware or software must be reported to a member of staff who will ensure that information is passed to relevant people such as Office Friends.

The School has filtering systems in place to block access to unsuitable material wherever possible to protect the welfare and safety of pupils. Pupils must not attempt to bypass this filter.

Viruses and malware can cause serious harm to the security of the School's network and that of others. Viruses and malware are often spread through internet downloads or circulated as attachments to emails / electronic communications. If pupils think or suspect that an attachment or other downloadable material might contain a virus or malware they must speak to the Teacher of ICT before opening the attachment or downloading the material.

Pupils must not disable or uninstall any anti-virus, anti-malware or pupil-monitoring software on the School's computers.

Appendix 2 use of Internet

Pupils must use the school's computer system for educational purposes only and are not permitted to access interactive or networking websites.

Pupils must take care to protect personal and confidential information about themselves and others when using the internet, even if the information is obtained inadvertently. Pupils understand that personal information such as full names, addresses, dates of birth and mobile numbers should not be put online.

Pupils should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights. Pupils must not breach copyright or plagiarise another's work.

Pupils must not load material from any external storage device brought in from outside the School onto the School's systems unless it has been authorised by the Teacher of ICT.

Pupils must not retrieve, download or share and illegal, offensive, potentially harmful or inappropriate material. Such material includes but is not limited to: content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, misogynistic / misandrist, homophobic, biphobic, pornographic, defamatory or relates to any form of bullying or sexual violence/ sexual harassment or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils must tell a member of staff if they have accidentally read, downloaded or have been sent any offensive material; or material which is inappropriate including personal information about anyone else.

Pupils must not communicate with staff using social networking sites or other internet or web- based communication channels unless this is expressively permitted for educational reasons.

Pupils should not bring the School into disrepute through their use of the internet.

Appendix 3 Other online communication by pupils

Anything pupils post on line whether through messaging, social media or by other means needs to be considered carefully. Pupils are reminded that there may be a 'disinhibition effect' making them more likely to post things that might be regretted later. The School may be involved in anything between pupils or anything which may bring the School into disrepute.

Pupils are advised to only post messages or images that they would be happy for a teacher, parent or guardian to see. They should avoid making strongly opinionated comments which could be deemed offensive. Pupils must also avoid making comments related to protected characteristics.

Anonymous posting is unwise. If pupils set up accounts to post anonymously (or that the presence of a group allows anonymity) all members of the group will be deemed individually responsible for material posted unless an individual admits responsibility. Nevertheless, other members of the group will be deemed partially responsible unless they have reported inappropriate posts or actively attempted to dissuade the perpetrator.

Pupils should not make comments about individuals online. Pupils are entitled to their opinions but the internet is not the place for such comments.

Pupils must never pose as anyone else or any institution.

Pupils must not harass others or post things intended to upset them. Do not troll.

Some messages and images may seem to be temporary and permanently deleted but this may not be the case if screen shots or photos are taken. Pupils are advised to treat all posts as permanent.

Pupils are advised to be cautious of meeting someone they have met online in real life. If a meeting is arranged for example someone belonging to a club, pupils should take an adult with them.

Pupils should remember that once you share something it can be freely and easily copied, shared or manipulated. Once you have shared it, you have lost control of it.

Pupils are advised against using ICT in bedrooms. It affects sleep and can make it more likely for them to post something they may regret. It best avoiding using ICT when tired.

Pupils are encouraged to think about how much ICT they use during a day. Use of the internet and gaming can both be addictive and it is difficult to self-regulate use.

Pupils are advised not to believe all they read online. Some sites publish dangerously inaccurate material. Pupils should be especially careful when investigating health concerns, sexuality, and identity and searching for supportive communities.

Appendix 4 Use of mobile electronic devices

Mobile electronic devices include but are not limited to: mobile phones, smartphones, tablets, laptops, MP3 players and wearable technology.

Pupils in years 7-10 are prohibited from having their mobile phones switched on during the School day. If they wish to make parental contact, they should request permission to use a school phone in the Main Office. Year 11 pupils must have their phones switched off except during the lunch break when they may be used in the Year 11 Area only.

Pupils in all year groups must leave their mobile phone in the classroom if using the lavatory during lesson time.

If any pupil uses their mobile phone without permission, it will be confiscated for the day and can only be collected at home time. Parents will be informed of phone misuse. Repeated offences may result in a pupil receiving a permanent ban from bringing mobile devices such as a mobile phone into School.

Mobile electronic devices must not be brought into the examination room under any circumstances, except where special arrangements for the use of a laptop have been agreed by the examinations Officer.

Pupils may use additional specified devices as part of a learning support plan only for the purposes stated in the plan and for examination Access arrangements.

Pupils should not communicate with staff using a mobile phone number except when this is expressly permitted by a member of staff for example if necessary, during an educational visit.

Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others or to share indecent images: consensually or non-consensually (including in chat groups) or to view or share pornography and other harmful or potentially harmful or inappropriate content will not be tolerated. This may also amount to a criminal offence. It will certainly be viewed as a serious breach of discipline whether or not the pupil is in the care of School at the time or not. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-bullying Policy and Behaviour and Discipline Policy). Pupils are encouraged to report inappropriate messages to a trusted adult.

The School does not accept any responsibility for the theft, loss of or damage to, mobile electronic devices brought onto the School premises including devices which have been confiscated or which have been handed in to staff.

Appendix 5 Photographs and Images

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Pupils may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with permission of those appearing in the image.

If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police.

If material found on the device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be handed to the police.

Pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. Staff will not view or forward illegal images of children.

The posting of images considered to be offensive or which brings the School into disrepute is a serious breach of of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Sharing nudes and semi-nude images and videos

'Sharing nudes and semi-nudes' means the consensual and non-consensual taking and sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 on line. This could be via social media, gaming platforms, chat apps or forums. It can also involve sharing devices offline e.g. via Apple's AirDrop. This may also be referred to as sexting or Youth produced sexual imagery.

Sharing or soliciting sexual images is strictly prohibited whether or not pupils are in the care of the School at the time that the image is recorded / shared. This includes the sharing of digitally manipulated or AI generated materials.

Sexting may be a criminal offence even if the picture is taken and shared with the permission of the person in the image. Even if a culprit is not prosecuted, this may result in information being stored on a police record which may prevent someone from working in certain jobs or travelling in the future.

The police may seize any devices which they believe may have been used for sexting. If the police find a device that contains inappropriate images they are unlikely to return it.

Pupils are asked to remember that once a photo or message is sent, they have no control about how it is passed on. Images shared online become public and may never be completely removed. They could be found in the future by anyone even by universities and future employers.

Even if pupils don't share images themselves, there is a risk that they may lose their device, it may be hacked or its data may still be accessible to a future owner.

Upskirting

Upskirting typically involves taking a picture under a person's clothing with out their permission / knowledge with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim distress, humiliation or alarm.

Upskirting is strictly prohibited whether or not a pupil is in the care of the School at the time the image is recorded.

Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do with something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a phone or camera but failing to do so due to lack of storage space or battery.

Appendix 6 Online sexual harassment

Online sexual harassment means ‘unwanted conduct of a sexual nature’ occurring online whether inside School or out of it.

The school takes a zero- tolerance approach to online sexual harassment. It is never acceptable and will not be tolerated. The School will treat incidents as a breach of discipline and will deal with them under the School’s behaviour and Discipline Policy and also as a safeguarding matter under the School’s child protection procedures (see the School’s Safeguarding and Child Protection Policy and procedures).

All allegations will be responded to seriously and all victims will be reassured and offered appropriate support, regardless of how long it has taken them to come forward and kept safe.

The School will consider online sexual harassment in broad terms, recognising that it can occur between 2 or more children of any age or sex and through a group of children sexually harassing a single child or group of children.

It will consider whether incidents of online sexual harassment are standalone or part of a wider pattern of sexual harassment / sexual violence. It may include:

- consensual and non-consensual sharing of nude and semi-nude images and / or videos;
- sexualised online bullying;
- unwanted sexual comments and messages, including on social media;
- sexual exploitation or coercion or threats; and
- coercing others into sharing images of themselves or performing acts they are not comfortable with online.

When dealing with online sexual harassment, staff will follow the School’s Safeguarding and Child protection Policy and procedures.

The Headteacher and staff authorised by her have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device contains illegal or undesirable material relating to online sexual harassment.

Appendix 7 harmful online challenges and online hoaxes

A hoax is a deliberate lie designed to seem truthful and online challenges generally involve users recording themselves taking a challenge or following a trend and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

If School becomes aware that harmful online challenges or online hoaxes are circulating between pupils, the School will handle this as a safeguarding matter under the School's child protection procedures.

The DSL will take a lead role in assessing the risk to the school community, undertake a case-by-case assessment including considering if the risk is a national one or localised to the area or just the School.

The factual basis of any harmful online challenge or online hoax will be checked through known reliable and trustworthy sources e.g. the Professional Online Safety Helpline, local safeguarding partners or local police force.

If, following investigation, the DSL finds that pupils have deliberately shared information with the intention of encouraging others to participate in harmful online challenges or online hoaxes, this will be treated as a breach of discipline and will be dealt with under the School's Behaviour and Discipline Policy.