Exeter School

Acceptable Use Policy (pupils)

Status:	Approved
Approver:	SLG
Source (author):	ALM
Last review date:	November 2025
Next review date:	November 2026

1 Aims

1.1 This is the acceptable use policy for pupils of Exeter School (**School)**, Department for Education number 878/6033 comprising:

1.1.1 the junior school for pupils in Year 3 to Year 6; and

1.1.2 the senior school for pupils in Year 7 to Year 13.

1.2 The aims of this policy are as follows:

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

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

(a) exposure to potentially illegal, harmful or inappropriate content (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact or conduct, including sexual harassment;

(d) cyberbullying and other forms of abuse; and

(e) online challenges and online hoaxes.

1.2.3 to minimise the risk of harm to the assets and reputation of the School;

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

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

1.2.6 to prevent the unnecessary criminalisation of pupils; and

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

1.3 This policy forms part of the School's whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the School and seeks to ensure that the best interests of pupils underpins and is at the forefront of all decisions, systems, processes and policies.

2 Scope and application

2.1 This policy applies to Exeter School. Please refer to the website for the separate policies for Exeter Pre-Prep School (Department for Education number 878/6046) including the Acceptable use policy for pupils of Exeter Pre-Prep School.

2.2 This policy applies to pupils 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 is put at risk.

2.3 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.

3 Regulatory framework

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

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Education and Skills Act 2008;

3.1.3 Children Act 1989;

3.1.4 Childcare Act 2006;

3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**); and

3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2025) (**KCSIE**);

3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Digital, Culture, Media & Sport (**DfDCMS**) and UK Council for Internet safety (**UKCIS**), March 2024);

3.2.4 Technical guidance for schools in England (Equality and Human Rights Commission, July 2024);

3.2.5 Searching, screening and confiscation: advice for schools (DfE, July 2022, in force from September 2022);

3.2.6 Behaviour in schools: advice for headteachers and school staff (DfE, February 2024)

3.2.7 Mobile phones in schools (DfE, February 2024)

3.2.8 Relationships education, relationships and sex education and health education guidance (DfE, September 2021).

3.2.9 Plan technology for your school (HM Government, September 2024);

3.2.10 Generative AI: product safety expectations (DfE, January 2025);

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

3.3.1 Behaviour management policy;

3.3.2 Anti-bullying policy;

3.3.3 Online safety policy;

3.3.4 Mobile phone use policy;

3.3.5 Safeguarding and child protection policy and procedures;

3.3.6 Relationships education / relationships and sex education policy; and

3.3.7 School rules.

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from School reception during the School day.

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

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to the **Proprietor** are references to the Board of Governors.

5.1.2 Reference to staff includes all those who work for or on behalf of the School, regardless of their employment status, including contractors, supply staff, volunteers and Governors unless otherwise indicated.

5.2 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 communications devices, network hardware and software and services and applications associated with them including:

5.2.1 the internet;

5.2.2 email;

5.2.3 electronic communications;

5.2.4 mobile phones and smart technology;

5.2.5 wearable technology;

5.2.6 desktops, laptops, netbooks, tablets / phablets;

5.2.7 personal music players;

5.2.8 devices with the capability for recording and / or storing still or moving images;

5.2.9 generative artificial intelligence technology / tools;

5.2.10 social networking, micro blogging and other interactive websites;

5.2.11 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;

5.2.12 webcams, video hosting sites (such as YouTube);

5.2.13 gaming sites;

5.2.14 virtual learning environments such as Microsoft Teams, Google Classroom or, Apple Classroom;

5.2.15 Interactive touchscreens including SMART boards;

5.2.16 other photographic or electronic equipment (e.g. GoPro device); and

5.2.17 devices which allow sharing services offline (e.g. Apple's AirDrop).

6 Responsibility statement and allocation of tasks

6.1 SLG has overall responsibility for all matters which are the subject of this policy.

6.2 To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	Head of IT Services	As required, and at least termly
Monitoring the use of technology across the School, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	Head of IT Services	As required, and at least termly
Monitoring the implementation of the policy, (including the record of incidents involving the use of technology (including through the use of generative AI) and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	IT Steering Group	As required, and at least termly
Online safety	Designated Safeguarding Lead	As required, and at least annually
Seeking input from interested groups (such as pupils, staff, parents) to consider improvements to the School's processes under the policy	IT Steering Group	As required, and at least annually
Formal annual review	SLG	Annually

7 Safe use of technology

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

7.2 The School has appropriate filtering and monitoring systems[1] in place to protect pupils using the internet (including email text messaging, social media sites and generative AI tools) when connected to the School's network, and their effectiveness is regularly reviewed. The School's approach to filtering and monitoring is set out in the Online safety policy.

7.3 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.

[1] Schools can use the DfE's 'plan technology for your school service' to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them.

The safe use of technology is integral to the School's curriculum and many of its policies and procedures. 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.

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

7.4.1 http://www.thinkuknow.co.uk/

7.4.2 https://www.childnet.com/young-people

7.4.3 https://www.saferinternet.org.uk/advice-centre/young-people

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

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

7.5 Please see the School's Online safety policy for further information about the School's online safety strategy.

7.6 Please see Appendix 4 for details of the School's response to online challenges and hoaxes.

8 Internet and email / electronic communication systems

8.1 The School provides internet, intranet access and an email to pupils to support their academic progress and development. Pupils are given individual usernames and passwords to access the School's internet, intranet and email system and these details must not be disclosed to any other person.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet and email / electronic communication systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

8.3 Staff and pupils may connect a personal device to the School network subject to this Agreement and the staff handbook. The use of any device connected to the School's network will be logged and monitored.

8.4 For the protection of all pupils, their use of email / electronic communication system and of the internet will be monitored by the School. Pupils should remember that even when an email / electronic message or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

8.5 The School uses a number of monitoring strategies to minimise safeguarding risks on internet connected devices, including:

8.5.1 physical monitoring by staff by watching screens of users;

8.5.2 live supervision by staff on a console with device management software;

8.5.3 network monitoring using log files of internet traffic and web access; and

8.5.4 individual device monitoring through software or third-party services.

9 School rules

9.1 Pupils **must** be aware of and observe rules and principles set out in the following Appendices:

9.1.1 The School's mobile phone policy;

9.1.2 The School's online safety policy;

9.1.3 communicating on-or-off-line using devices, apps, platforms, and email (Appendix 1);

9.1.4 photographs and images (including the consensual and non-consensual sharing of nude and semi-nude images and videos) (Appendix 2);

9.1.5 online sexual harassment (Appendix 3); and

9.1.6 harmful online hoaxes and challenges (Appendix 4).

9.2 The purpose of these rules is to set out the principles which pupils must act in accordance with and the rules which pupils must follow to use technology safely and securely.

9.3 These principles and rules apply to all use of technology, whether during or outside of school.

10 Procedures

10.1 The way in which pupils relate to one another online can have a 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 be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils they should report it to a teacher immediately.

10.2 Any misuse of technology by pupils will be dealt with under the School's Behaviour management policy and, where safeguarding concerns are raised, under the Safeguarding and child protection policy and procedures.

10.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology, including cyberbullying, prejudiced-based bullying and discriminatory bullying will be dealt with under the School's Anti-bullying policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's Anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

10.4 The School has adopted a zero-tolerance approach to sexual violence and sexual harassment - it is never acceptable, and it 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, an unsafe environment for children and, in worst case scenarios, a culture that normalises abuse.

10.5 Sexual harassment, in the context of this policy, means "unwanted conduct of a sexual nature" and the School recognises that this can occur both online and offline. Pupils must not use their own or the School's technology to sexually harass others at any time, whether during or outside of school. Incidents of sexual harassment involving the use of technology will be dealt with under the School's Behaviour management 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 about it as soon as possible.

10.6 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"[2] and the School is aware that this can occur online and / or face-to-face and can also occur simultaneously between the two.

10.7 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 an assurance of confidentially in relation to their concern as information may need to shared further (e.g. with the School's Designated Safeguarding Lead) to consider next steps. See Appendix 3 for further information.

10.8 The Designated Safeguarding Lead takes lead responsibility within the School for safeguarding and child protection, including online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Safeguarding and child protection policy and procedures).

10.9 If a pupil is worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a teacher about it as soon as possible.

10.10 The School is also aware of the risk 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 Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.[3] Any person who has a concern relating to extremism may report it directly to the police.

10.11 **Cybercrime**

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

10.11.2 Cyber-dependent crimes include:

(a) unauthorised access to computers (illegal "hacking"), such as accessing a school's computer network to look for test answers or change grades awarded;

(b) denial of service (**DoS** or **DDoS**) attacks or "booting", which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

[2] The Lucy Faithful Foundation has developed a HSB toolkit which provides support, advice and information on how to prevent HSB which schools may find helpful.
[3] See Channel and Prevent Multi-Agency Panel (PMAP) guidance for more information

(c) making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

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

10.11.4 The School will take appropriate action to meet the Cyber security standards to improve resilience against cyber-attacks.

10.11.5 Any concerns about a pupil in this area will be referred to the Designated Safeguarding Lead immediately. The Designated Safeguarding Lead will then consider referring into 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.

10.12 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead in relation to pupils and the Head of HR in relation to staff (who may in turn refer the matter to the DSL). Incidents will be recorded in CPOMS for pupils and personnel files for staff.

11 Sanctions

11.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Proprietor has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour management policy including, in the most serious cases, permanent exclusion. Any action taken will depend on the seriousness of the offence.

11.2 Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and the School's Behaviour management policy (see Appendix 6 of the Behaviour management policy for the School's policy on the searching and confiscation of electronic devices).

11.3 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 a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 2 for more information on photographs and images.

11.4 The School reserves the right to charge a pupil or his / her parents for any costs incurred to the School as a result of a breach of this policy.

12 Training

12.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that all staff, including supply staff volunteers and Governors:

12.1.1 understand what is expected of them by this policy; and

12.1.2 have the necessary knowledge and skills to carry out their roles; and

12.1.3 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.

12.2 Staff training is regularly updated, and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation, dealing with harmful online challenges and online hoaxes and on the risks associated with generative AI tools and content created by them. This training may be in addition to the regular safeguarding and child protection (including online safety) updates as required at induction and at least annually thereafter.

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

12.4 The School maintains written records of all staff training.

13 Risk assessment

13.1 The School recognises that technology, and the risks and harms 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 assessments where appropriate which consider and reflect the risks faced by their pupils.

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

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

13.4 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

13.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to the DSL or DDSLs who have been properly trained in, and tasked with, carrying out the particular assessment.

14 Record keeping

14.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

14.2 All serious incidents involving the use of technology will be logged centrally in CPOMS and any matters of safeguarding concern will be brought to the attention of the Designated Safeguarding Lead in accordance with the School's safeguarding and child protection policy and procedures.

14.3 The records created in accordance with this policy may contain personal data. The School's use of this personal data will be in accordance with data protection law. The School has published on its website privacy notices which explain how the School will use personal data.

Appendix 1 Use of the internet and email / electronic communication services

1 The School does not undertake to provide continuous internet access. Email / electronic communication services and website addresses at the School may change from time to time.

Use of the internet

2 You must use the School's computer system for educational purposes only.

3 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

4 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the Head of IT Services.

5 You 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 - you must not copy (plagiarise) another's work.

6 You must not view, retrieve, download or share any 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 that 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. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

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

8 You must not bring the School into disrepute through your use of the internet.

Use of email / electronic communication services

9 Pupils in years 3 to 11 must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail or electronic communication devices, apps or platforms through the School's network. This will be unnecessary as you are provided with your own individual email account for School purposes.

10 Pupils in years 12 and 13 may use any personal devices and services, including personal web-based email accounts within the times and locations specified by the School in accordance with the mobile phone policy and must continue to use only their school provided email account for communicating with members of staff.

11 Your School email / electronic communication accounts can be accessed from home using your School-issued Office365 account. The School will not forward messages received during the School holidays.

12 You must use your School email / electronic communication accounts (e.g. the chat functionality of Microsoft Teams or Google Classroom, virtual learning environment, homework submission tool etc) as the only mean(s) of electronic communication with staff. Communication either from a personal account or to a member of staff's personal account is not permitted.

13 Email / electronic communications should be treated in the same way as any other forms of written communication. You should not include or ask to receive anything in a message which is not appropriate to be published generally or which you believe the Head and / or your parent would consider to be inappropriate. Remember that messages could be forwarded to or seen by someone you did not intend.

14 You must not send or search for any messages which contain 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, indecent, defamatory or that relates to any form of bullying or sexual violence / sexual harassment or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must inform a member of staff as soon as possible. Use of the email / electronic messaging system in this way is a serious breach of discipline and may constitute a criminal offence.

15 Trivial messages and jokes should not be sent or forwarded through the School's email / electronic communication systems. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the School's network to suffer delays and / or damage.

16 You must not use the School's email / electronic communication systems to send misogynistic messages or messages which contain language relating to sexual violence or which could be interpreted as being harassment, whether of a sexual nature or otherwise. The School has adopted a zero-tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a serious breach of discipline and will deal with them under the School's Behaviour management policy and also as a safeguarding matter under the School's Safeguarding and child protection policy and procedures.

17 All correspondence from your School account must contain the School's disclaimer.

18 You must not read anyone else's messages without their consent.

Appendix 2 Photographs and images

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

2 You 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 the 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, as stated in paragraph 11.3 of this policy.

3 If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

4 You 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 a child.

5 The posting of images which in the reasonable opinion of the Head is considered to be offensive or which brings the School into disrepute is a serious breach 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.

6 **Sharing nude and semi-nude images and videos**

6.1 "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 online, including the sharing of digitally manipulated or AI-generated nude and semi-nude images. This could be via social media, gaming platforms, chat apps or forums. It can also involve sharing between devices offline e.g. via Apple's AirDrop. This may also be referred to as sexting or youth produced sexual imagery.

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

6.3 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 you are not prosecuted, this may result in information being stored on your police record, which may prevent you from doing certain jobs in the future.

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

6.5 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

6.6 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.

6.7 Even if you don't share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

6.8 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding and child protection policy and procedures).

6.9 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

6.10 If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

7 Upskirting

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

7.2 Upskirting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded.

7.3 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 something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

7.4 The School will treat incidences of upskirting as a serious breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding and child protection policy and procedures).

7.5 If you are concerned that you have been a victim of upskirting, speak to any member of staff for advice.

Appendix 3 Online sexual harassment

1 Online sexual harassment means "unwanted conduct of a sexual nature" occurring online, whether in School or outside of it.

2 The School takes a zero-tolerance approach to online sexual harassment, and it is never acceptable and it will not be tolerated. The School will treat incidences as a serious breach of discipline and will deal with them under the School's Behaviour management 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).

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

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

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

5.1 consensual and non-consensual sharing of nude and semi-nude images and / or videos;

5.2 sexualised online bullying;

5.3 unwanted sexual comments and messages, including on social media;

5.4 sexual exploitation, coercion or threats; and

5.5 coercing others into sharing images of themselves or performing acts they're not comfortable with online.

6 If you are concerned that you or someone else have been a victim of online sexual harassment, speak to any member of staff for advice.

7 When dealing with online sexual harassment staff will follow the School's Safeguarding and child protection policy and procedures.

8 The Head and staff authorised by them 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. The School's search procedures can be found in the School's Behaviour management policy.

Appendix 4 Harmful online challenges and online hoaxes

1 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.

2 If the 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 (see the School's Safeguarding and child protection policy and procedures).

3 The Designated Safeguarding Lead 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.

4 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.

5 If, following investigation, the Designated Safeguarding Lead 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 serious breach of discipline and will be dealt with under the School's Behaviour management policy.

6 The Head and staff authorised by them 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 is being used to commit an offence or cause personal injury or damage to property. The School's search procedures can be found in the school Behaviour management policy.

Appendix 5 Generative artificial intelligence

7 The School recognises the increasing presence of generative artificial intelligence (**AI**) technology. Although generative AI is not new, recent advances mean this technology is easily available to pupils to produce AI-generated content such as text, audio, code, images and video simulations.

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

a. AI and human intelligence are not the same: AI tools do not understand what they produce or the impact the generated content may have;

b. sometimes AI tools will generate answers that sound plausible but they may not be correct;

c. content produced may perpetuate harmful biases and stereotypes and may not be age-appropriate;

d. over-reliance on these tools will reduce opportunities to improve research skills, writing and critical thinking;

e. AI tools store and learn information submitted to them so personal data[4] should never be entered;

f. if teachers indicate that pupils are permitted to use generative AI technologies in their work, pupils must observe all related instructions and guidance; and

g. submitting work produced in whole or part by AI without proper referencing or acknowledging use of AI may be considered cheating and inappropriate use of AI.

9 Any misuse or inappropriate use of AI technologies by pupils will be addressed in accordance with the School's disciplinary policies and procedures.

10 The School will implement measures to ensure the safe and appropriate use of AI technologies within its network. These measures include ensuring that any generative AI tools used by pupils effectively and reliably prevent access to illegal, harmful and inappropriate content and ensuring that the generative AI tool has robust activity logging procedures to allow efficient monitoring of AI activities. The School will restrict access to certain AI systems if they are not considered safe for pupils and may provide guidelines on the use of specific AI applications.

[4] Personal data is any information that relates to an identified or identifiable living individual. An individual does not have to be named in the information for it to be their personal data, provided it is possible to work out that the information relates to them using means reasonably likely to be used. Therefore removing names from information is not always enough to prevent it from being personal data.