



THE KING'S SCHOOL

GRANTHAM

Acceptable Use Policy for Pupils

Contents

Clause

1	Aims	2
2	Scope and application	2
3	Regulatory framework	2
4	Publication and availability	3
5	Definitions	3
6	Responsibility statement and allocation of tasks	4
7	Safe use of technology	5
8	Internet and email / electronic communication systems	6
9	Behaviour expectations	6
10	Procedures	6
11	Sanctions	7
12	Training	7
13	Risk assessment	7
14	Record keeping	8
15	Version control	8

Appendix

Appendix 1	Access and security	9
Appendix 2	Use of the internet and email / electronic communication services.....	10
Appendix 3	Use of mobile electronic devices.....	12
Appendix 4	Photographs and images.....	13
Appendix 5	Online sexual harassment.....	15
Appendix 6	Harmful online challenges and online hoaxes	16

1 **Aims**

- 1.1 This is the acceptable use policy for pupils of The King's School (**Academy**).
- 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 harmful or inappropriate material (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 Academy;
 - 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 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 culture of safety, equality and protection.

2 **Scope and application**

- 2.1 This policy applies to the whole Academy.
- 2.2 This policy applies to the use of technology at all times when a pupil is:
 - 2.2.1 in or at the Academy;
 - 2.2.2 representing the Academy or wearing School uniform;
 - 2.2.3 travelling to or from the Academy;
 - 2.2.4 on Academy-organised trips; or
 - 2.2.5 associated with the Academy at any time.
- 2.3 This policy shall also apply to pupils at all times and places in circumstances where failing to apply this policy may:
 - 2.3.1 affect the health, safety or well-being of a member of the Academy community or a member of the public;
 - 2.3.2 have repercussions for the orderly running of the Academy; or
 - 2.3.3 bring the Academy into disrepute.
- 2.4 Parents are encouraged to read this policy with their child. The Academy actively promotes the participation of Parents to help the Academy 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 Academy's responsibilities under:

- 3.1.1 Education (Independent School Standards) Regulations 2014;
 - 3.1.2 Education and Skills Act 2008;
 - 3.1.3 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR); and
 - 3.1.4 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 2021) (**KCSIE**);
 - 3.2.2 [Working together to safeguard children](#) (DfE, July 2018, as amended December 2020);
 - 3.2.3 [Prevent duty guidance for England and Wales](#) (Home Office, April 2021)
 - 3.2.4 [Channel duty guidance: protecting vulnerable people from being drawn into terrorism](#) (Home Office, 2020);
 - 3.2.5 [Preventing and tackling bullying: advice for headteachers, staff and governing bodies](#) (DfE, July 2017);
 - 3.2.6 [Advice and Guidance: How can we stop prejudice-based bullying in schools?](#) (Equality and Human Rights Commission);
 - 3.2.7 [Information sharing: advice for practitioners providing safeguarding services to children, young people, parents and carers](#) (DfE, July 2018);
 - 3.2.8 [Sexual violence and sexual harassment between children in schools and colleges](#) (DfE, May 2018);
 - 3.2.9 [Relationships Education, Relationships and Sex Education \(RSE\) and Health Education guidance](#) (DfE, July 2019).
- 3.3 The following Academy policies, procedures and resource materials are relevant to this policy:
- 3.3.1 Behaviour and Discipline Policy;
 - 3.3.2 Anti-Bullying Policy;
 - 3.3.3 Online Safety Policy;
 - 3.3.4 Safeguarding and Child Protection Policy and Procedures;
 - 3.3.5 Relationships and Sex Education Policy.

4 **Publication and availability**

- 4.1 This policy is published on the Academy website.
- 4.2 This policy is available in hard copy on request.
- 4.3 A copy of the policy is available for inspection from The PA to the Head Master 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 **Parent** or **Parents** means the natural or adoptive Parents of the pupil (irrespective of whether they are or have ever been married, with whom the pupil lives, or whether they have contact with the pupil) as well as any person who is not the natural or adoptive Parent of the pupil, but who has care of, or Parental responsibility for, the pupil (e.g. foster carer / legal guardian).
 - 5.1.2 References to the **Proprietor** are references to The King's School the Academy Trust.

- 5.1.3 References to **school days** mean Monday to Friday, when the Academy is open to pupils during term time. The dates of terms are published on the Academy's website.
- 5.2 The Academy will take a wide and purposive approach to considering what falls within the meaning of **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 smartphones;
 - 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 social networking, micro blogging and other interactive websites;
 - 5.2.10 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;
 - 5.2.11 webcams, video hosting sites (such as YouTube);
 - 5.2.12 gaming sites;
 - 5.2.13 virtual learning environments such as The King's School SharePoint site;
 - 5.2.14 SMART boards; and
 - 5.2.15 other photographic or electronic equipment e.g. GoPro devices; and
 - 5.2.16 devices which allow sharing services offline e.g. Apple's AirDrop.

6 **Responsibility statement and allocation of tasks**

- 6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy.
- 6.2 The Proprietor is aware of its duties under the Equality Act 2010 and the requirement under s.149 of the Equality Act 2010 to meet the Public Sector Equality Duty. This means in carrying out its functions, the Proprietor is required to have due regard to the need to:
- 6.2.1 eliminate discrimination and other conduct that is prohibited by the Act;
 - 6.2.2 advance equality of opportunity between people who share a protected characteristic and people who do not share it; and
 - 6.2.3 foster good relations across all characteristics - between people who share a protected characteristic and people who do not share it.
- 6.3 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	The Head Master	As a minimum annually, ideally termly, and as required
Monitoring the use of technology across the	The Deputy Head Master (Pastoral)	As a minimum annually, ideally termly, and as required

Task	Allocated to	When / frequency of review
Academy, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change		
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness	The Head Master	As a minimum annually, ideally termly, and as required
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the UK GDPR	The Head Master	As required, and at least termly
Online safety	Designated Safeguarding Lead	As required, and at least termly
Formal annual review	Proprietor	As a minimum annually, and as required
Overall responsibility for content and implementation	Proprietor	As a minimum 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 Academy 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 Academy's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.
- 7.3 Pupils may find the following resources helpful in keeping themselves safe online:
- 7.3.1 <http://www.thinkuknow.co.uk/>
 - 7.3.2 <https://www.childnet.com/young-people>
 - 7.3.3 <https://www.saferinternet.org.uk/advice-centre/young-people>
 - 7.3.4 <https://www.disrespectnobody.co.uk/>
 - 7.3.5 <http://www.safetynetkids.org.uk/>
 - 7.3.6 <https://www.childline.org.uk/>
 - 7.3.7 <https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/>
 - 7.3.8 <https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people>

- 7.4 Please see the Academy's Online Safety Policy for further information about the Academy's online safety strategy.
- 7.5 Please see Appendix 6 for details of the Academy's response to online challenges and hoaxes.
- 8 Internet and email / electronic communication systems**
- 8.1 The Academy provides internet access and an email / electronic communication system (for example Microsoft 365 suite) to pupils to support their academic progress and development.
- 8.2 Pupils may only access the Academy's network when given specific permission to do so. All pupils will receive guidance on the use of the Academy's SharePoint, Teams and email 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 For the protection of all pupils, their use of email / electronic communication system and of the internet will be monitored by the Academy. 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 in the cloud, on servers or storage media are always private.
- 9 Behaviour expectations**
- 9.1 Pupils must be aware of the behaviour expectations and observe the rules and expectations set out in the following Appendices and as required by the Academy's Behaviour and Discipline Policy.
- 9.1.1 access and security (Appendix 1);
- 9.1.2 communicating on-or-off-line using devices, apps, platforms, and email (Appendix 2);
- 9.1.3 use of mobile electronic devices (Appendix 3);
- 9.1.4 photographs and images (including "sexting") (Appendix 4);
- 9.1.5 online sexual harassment (Appendix 5); and
- 9.1.6 harmful online hoaxes and challenges (Appendix 6).
- 9.2 The purpose of these rules and expectations 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.
- 9.3 These expectations and rules apply to all use of technology.
- 10 Procedures**
- 10.1 Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher about it as soon as possible.
- 10.2 Any misuse of technology by pupils will be dealt with under the Academy's Behaviour and Discipline 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 Academy's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the Academy'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 Academy's Anti-Bullying Policy for further information about cyberbullying and e-safety, including useful resources.
- 10.4 Pupils must not use their own or the Academy's technology to sexually harass others. Incidents of sexual harassment involving the use of technology will be dealt with under the Academy's Behaviour and Discipline and Safeguarding and Child Protection Policies and

Procedures. 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. See Appendix 5 for further information.

- 10.5 The Designated Safeguarding Lead takes lead responsibility within the Academy for safeguarding and child protection, including online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the Academy's child protection procedures (see the Academy's Safeguarding and Child Protection Policy and Procedures).
- 10.6 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.
- 10.7 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.
- 10.8 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 who will record the matter centrally.

11 Sanctions

- 11.1 Where a pupil breaches any of the School policies behaviour expectations, practices or procedures set out in this policy or the appendices, the Proprietor has authorised the Head Master to apply any sanction which is appropriate and proportionate to the breach in accordance with the Academy's Behaviour and Discipline Policy including, in the most serious cases, a fixed term exclusion or permanent exclusion. Other sanctions might include: increased monitoring procedures; withdrawal of the right to access the Academy's internet and email / electronic communication facilities; detention. 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 Academy's Behaviour and Discipline Policy (see the Behaviour and Discipline Policy for the Academy'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 4 for more information on photographs and images.

12 Training

- 12.1 The Academy ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that staff and volunteers understand what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.
- 12.2 The level and frequency of training depends on role of the individual member of staff.
- 12.3 The Academy maintains written records of all staff training.

13 Risk assessment

- 13.1 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.
- 13.2 The format of risk assessment may vary and may be included as part of the Academy'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 Academy's approach to promoting pupil welfare will be systematic and pupil focused.

- 13.3 The Head Master 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.
- 13.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to The Deputy Head Master and the Heads of Year who have/has 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 Academy'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 by the Designated Safeguarding Lead.

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

15 Version control

Date of adoption of this policy	September 2021
Date of last review of this policy	September 2021
Date for next review of this policy	September 2022

Appendix 1 Access and security

- 1 Access to the internet from the Academy's computers and network must be for educational purposes only. You must not use the Academy's facilities or network for personal, social or non-educational use without the express, prior consent of a member of staff.
- 2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the Academy's or any other computer system, or any information contained on such a system.
- 3 No laptop or other mobile electronic device may be connected to the Academy network without the consent of member of staff.

The use of cellular data (e.g. GPRS, 3G, 4G, 5G etc) to access the internet while pupils are on Academy premises or otherwise in the care of the Academy is discouraged, as pupils are unable to benefit from the Academy's filtering and anti-virus software. Pupils accessing the internet outside the Academy's network whilst on Academy premises or otherwise in the care of the Academy do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

- 4 Passwords protect the Academy's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.
- 5 You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact IT Support.
- 6 You must not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.
- 7 The Academy has a firewall in place to ensure the safety and security of the Academy's networks. You must not attempt to disable, defeat or circumvent any of the Academy's security facilities. Any problems with the firewall must be reported to the class teacher or IT Support.
- 8 The Academy has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.
- 9 Viruses can cause serious harm to the security of the Academy's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails / electronic communications. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to IT Support before opening the attachment or downloading the material.
- 10 You must not disable or uninstall any anti-virus software on the Academy's computers.
- 11 The use of location services represents a risk to the personal safety of pupils and to Academy security. The use of any website or application, whether on an Academy or personal device, with the capability of identifying the user's location while you are on Academy premises or otherwise in the care of the Academy is discouraged.

Appendix 2 Use of the internet and email / electronic communication services

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

Use of the internet

- 2 You must use the Academy's computer system for educational purposes only and are not permitted to access interactive or networking websites without the express, prior consent of a member of staff.
- 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 Academy onto the Academy's systems, unless this has been authorised by the IT Support.
- 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 offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory 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 Academy into disrepute through your use of the internet.

Use of email / electronic communication services

- 9 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail or electronic communication devices, apps or platforms through the Academy's network without the express, prior consent of a member of staff. This will be unnecessary as you are provided with your own personal email account for Academy purposes.
- 10 Your Academy email can be accessed from home.
- 11 You must use your Academy email / electronic communication accounts [e.g. the chat functionality of MS Teams, virtual learning environment, 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.
- 12 Email / electronic communications should be treated in the same way as any other form 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 Master and / or your Parents would consider to be inappropriate. Remember that messages could be forwarded to or seen by someone you did not intend.

- 13 You must not send or search for any messages which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory 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.
- 14 Trivial messages and jokes should not be sent or forwarded through the Academy's email / electronic communication systems. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the Academy's network to suffer delays and / or damage.
- 15 All correspondence from your Academy email account must contain the Academy's disclaimer.
- 16 You must not read anyone else's messages without their consent.

Appendix 3 Use of mobile electronic devices

- 1 **Mobile electronic device** includes but is not limited to mobile phones, smartphones, tablets, laptops and MP3 players and wearable technology.
- 2 Mobile phones and other mobile electronic devices must be switched off or on silent mode and kept out of sight during School hours, including at break times and between lessons. Use of such devices is only permitted during School hours with the express permission of a member of staff or in form rooms at lunch time. Sixth Form students may use mobile devices in the Sixth Form Centre.

The use of cellular data (e.g. GPRS, 3G, 4G, 5G etc) to access the internet while pupils are on Academy premises or otherwise in the care of the Academy is discouraged, as pupils are unable to benefit from the Academy's filtering and anti-virus software. Pupils accessing the internet outside the Academy's network whilst on Academy premises or otherwise in the care of the Academy do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.
- 3 The use of mobile phones during the Academy day will not be necessary. In emergencies, you may request to use the Academy telephone. Should your Parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.
- 4 You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Head Master in writing.
- 5 You must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.
- 6 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the Academy at the time of such use. Appropriate disciplinary action will be taken where the Academy becomes aware of such use (see the Academy's Anti-Bullying Policy and Behaviour and Discipline Policy) and the Academy's safeguarding procedures will be followed in appropriate circumstances (see the Academy's Safeguarding and Child Protection Policy and Procedures).
- 7 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the Academy's Behaviour and Discipline Policy on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the Academy temporarily or permanently and at the sole discretion of the Head.
- 8 The Academy does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto Academy premises, including devices that have been confiscated or which have been handed in to staff.

Sanctions

Mobile phones must be switched to silent and out of sight at all times. If a phone rings or is seen by a member of staff, or if inappropriate use is made of the phone, it will be confiscated.. Confiscated phones should be handed to the Head Master's PA. A record of the offence will be kept and recorded on SIMS.

Students are required to explain this to parents and the phone will only be returned to parents. If the offence is repeated the phone will be confiscated, only returned to parents and an after-school detention issued with a member of SLT. Should the offence be repeated a third time the student may not bring a mobile phone to school at any time. The student will also receive an internal exclusion.

Appendix 4 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.
- 5 The posting of images which in the reasonable opinion of the Head Master is considered to be offensive or which brings the Academy 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 Academy or personal facilities.
- 6 **Sharing nude and semi-nude images and videos**
 - 6.1 "Sharing nudes and semi-nudes" means the taking and sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. 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 sexual images is strictly prohibited, whether or not you are in the care of the Academy at the time the image is recorded and / or shared.
 - 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 Academy 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 Academy'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 them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, 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 Academy will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the Academy's child protection procedures (see the Academy'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 5 Online sexual harassment

- 1 Online sexual harassment means "unwanted conduct of a sexual nature" occurring online.
- 2 Online sexual harassment is never acceptable and it will not be tolerated. The Academy will treat incidences as a breach of discipline and will deal with them under the Academy's Behaviour and Discipline Policy and also as a safeguarding matter under the Academy's safeguarding and child protection procedures (see the Academy's Safeguarding and Child Protection Policy and Procedures).
- 3 All allegations will be responded to seriously and all victims will be offered appropriate support, regardless of how long it has taken for them to come forward.
- 4 The Academy 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 non-consensual sharing of nude and semi-nude images and videos sexual images;
 - 5.2 sexualised online bullying;
 - 5.3 unwanted sexual comments and messages, including on social media; and
 - 5.4 sexual exploitation, coercion or threats.
- 6 If you are concerned that you 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 Academy's Safeguarding and Child Protection Policy and Procedures).
- 8 The Head Master and staff authorised by them have a statutory power to search pupils / property on academy 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 Academy's search procedures can be found in the Academy Behaviour and Discipline Policy.

Appendix 6 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, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.
- 2 If the Academy becomes aware that harmful online challenges or online hoaxes are circulating between pupils, the Academy will handle this as a safeguarding matter under the Academy's safeguarding and child protection procedures (see the Academy's Safeguarding and Child Protection Policy and Procedures).
- 3 The DSL will take a lead role in assessing the risk to the Academy community, undertake a case-by-case assessment, including considering if the risk is a national one or localised to the area, or just the Academy.
- 4 The factual basis of any harmful online challenge or online hoax will be checked through reliable sources e.g. the Professional Online Safety Helpline, local safeguarding partners or local police force.
- 5 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 Academy's Behaviour and Discipline Policy.
- 6 The Head Master and staff authorised by them have a statutory power to search pupils / property on academy 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 Academy's search procedures can be found in the Academy's Behaviour and Discipline Policy.