THE KING'S SCHOOL

GRANTHAM

Acceptable Use Policy for Pupils

Contents

Appendix

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 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 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 child-to-child risks when using technology;

1.2.6 to create a calm, safe and supportive environment free from disruption in which pupils can thrive and flourish both in and out of the classroom and reach their full potential;

1.2.7 to create, promote and maintain high expectations of good behaviour amongst pupils through a whole school approach to behaviour;

1.2.8 to prevent the unnecessary criminalisation of pupils; and

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

1.3 This policy forms part of the Academy's whole school approach to promoting child safeguarding and wellbeing, which involves everyone at the Academy 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 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 off Academy premises including

(a) representing the Academy or wearing School uniform;

(b) travelling to or from the Academy;

(c) on Academy-organised trips; or

(d) 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), as amended by the Data Protection and Digital Information Act 2025; 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 2025) (**KCSIE**);

3.2.2 Working together to safeguard children (HM Government, updated February 2024) (**WTSC**);

3.2.3 Prevent duty guidance for England and Wales (HM Government, in force December 2023);

3.2.4 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, December 2023);

3.2.5 Sharing nudes and semi-nudes: advice for education settings working with children and young people (DCMS and UKCIS, March 2024);

3.2.6 Preventing and tackling bullying: advice for headteachers, staff and governing bodies (DfE, July 2017);

3.2.7 Searching, screening and confiscation: advice for schools (DfE, July 2023);

3.2.8 Information sharing: advice for practitioners providing safeguarding services to children, young people, parents and carers (HM Government, May 2024);

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

3.2.10 Mobile phones in schools (DfE, February 2024);

3.2.11 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, September 2021).

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

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

5.1.4 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, 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 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 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 The King's School SharePoint site;

5.2.15 SMART boards; and

5.2.16 other photographic or electronic equipment e.g. GoPro devices; and

5.2.17 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	As a minimum annually, ideally termly, and as required
Monitoring the use of technology across the Academy, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	The Deputy Head (Pastoral)	As a minimum annually, ideally termly, and as required
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	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	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 and many of its policies and procedures. Staff are aware that technology can be a significant component in many safeguarding and wellbeing issues. 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.childline.org.uk/

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

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. Pupils are given individual usernames and passwords to access the Academy's internet, intranet and email system and these details must not be disclosed to any other person.

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/ electronic communications 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 No laptop or other mobile electronic device may be connected to the Academy network without the consent of the School Business Leader or the Head. The use of any device connected to the Academy's network will be logged and monitored by the Deputy Head Master.

8.4 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.

8.5 The Academy uses a SmoothWall filtering and monitoring system to protect pupils. Its effectiveness is reviewed regularly in line with **KCSIE 2025** and **DfE Filtering and Monitoring Standards (2023)**, with outcomes reported to the Senior Leadership Team.

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 Academies Behaviour 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 and smart technology (Appendix 3);

9.1.4 photographs and images (including the consensual and non-consensual sharing of nude and semi-nude images and videos) (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 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 significant impact on the Academy'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 talk to a teacher about it immediately.

10.2 Any misuse of technology by pupils will be dealt with under the Academy's Behaviour 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, including cyberbullying, prejudiced-based bullying and discriminatory bullying, 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 The Academy 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" as the Academy recognises that this can occur both online and offline. Pupils must not use their own or the Academy'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 Academy's Behaviour 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.

10.6 The Academy 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" and the Academy is aware that this can occur online and/ or face-to-face and can occur simultaneously between the two.

10.7 Any reports of sexual violence or sexual harassment will be taken extremely seriously by the Academy 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 Academy's Designated Safeguarding Lead) to consider next steps. See Appendix 5 for further information.

10.8 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.

10.9 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 Academy 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 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.

10.11 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 off-line but are enabled at scale and at speed on-line) 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'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;

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

(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 Academy 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 Any concerns about a pupil in this area will be referred to the DSL immediately. The DSL will consider referral to the **Cyber Choices programme** and, where appropriate, involve law enforcement in line with the **Computer Misuse Act 1990** and **National Crime Agency guidance**. 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 who will record the matter centrally in the technology incidents log.

11 Generative Artificial Intelligence

11.1 The Academy 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.

11.2 When using any generative AI technologies pupils must also comply with the school's academic integrity rules and intellectual property law.

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

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

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

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

11.3.4 AI tools store and learn information submitted to them so personal or sensitive information should never be entered;

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

11.3.6 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.

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

11.5 The Academy 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.

12 Sanctions

12.1 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 to apply any sanction which is appropriate and proportionate to the breach in accordance with the Academy's Behaviour Policy including, in the most serious cases, a suspension 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.

12.2 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 Policy (see the Behaviour Policy for the Academy's policy on the searching and confiscation of electronic devices).

12.3 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.

13 Training

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

13.1.1 understand what is expected of them by this policy;

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

13.1.3 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.

13.2 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 and dealing with harmful online challenges and online hoaxes. 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.

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

13.4 The Academy maintains written records of all staff training.

14 Risk assessment

14.1 The Academy recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The Academy will carry out regular, and at least annual, reviews of its approach to online safety, supported by risk assessments which consider and reflect the risks face by their pupils.

14.2 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.

14.3 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.

14.4 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.

14.5 Day to day responsibility to carry out risk assessments under this policy will be delegated to The Deputy Head and the Heads of Year who have/has been properly trained in, and tasked with, carrying out the particular assessment.

15 Record keeping

15.1 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.

15.2 All serious incidents involving the use of technology will be logged centrally by the Designated Safeguarding Lead in the technology incident log and the Head informed.

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.

16 Version control

Date of adoption of this policy	September 2021
Date of last review of this policy	February 2025
Date for next review of this policy	October 2025
Policy owner (SMT)	Justin Dixon

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 OR 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 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, or that relates to any form of bullying, or sexual violence/sexual harassment, biphobic, 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 by Office 365.

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 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 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 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, biphobic, homophobic, relates to any form of bullying, sexual violence/sexual harassment, pornographic, indecent, 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 You must not use the Academy'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 Academy has adopted a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The Academy will treat any such incidences as a breach of discipline and will deal with them under the Academy's Behaviour Policy and also as a safeguarding matter under the Academy's Safeguarding and child protection Policy and procedures.

16 All correspondence from your Academy email account must contain the Academy's disclaimer.

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

Appendix 3 Use of mobile electronic devices and smart technology

1 **Mobile electronic device** includes but is not limited to mobile phones, smartphones or other smart technology, 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 for academic purposes. Sixth Form students may use mobile devices in the Sixth Form Centre. In certain circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the Academy's network. Express permission to do so must be sought and given from a member of staff in advance.

3 The Academy does all that it reasonably can to limit pupils' exposure to potentially harmful and inappropriate material online through the use of the Academy's IT system. The Academy has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when connected to the Academy's network, and their effectiveness is regularly reviewed.

4 The Academy acknowledges that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). and is aware that this means that some children, whilst at school, may sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

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.

5 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.

6 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 in writing.

7 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.

8 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others or to share indecent images: consensually and non-consensually (including in large chat groups) or to view and share pornography and other harmful or potentially harmful or inappropriate content 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 Policy) and the Academy's safeguarding procedures will be followed in appropriate circumstances (see the Academy's Safeguarding and Child Protection Policy and Procedures).

9 Pupils must not use their mobile and smart technology to send abusive, racist, sexist , homophobic, biphobic, pornographic, indecent, defamatory, misogynistic / misandrist 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, or considered to be an extreme or terrorist related nature. The Academy has adopted a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The Academy will treat any such incidences as a breach of discipline and will deal with them under the Academy's Behaviour policy and also as a safeguarding matter under the Academy's Safeguarding and Child Protection Policy and rocedures.

10 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.

11 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

12 Where staff confiscate a mobile phone that has been used without staff permission in a lesson or around the school, Staff will confiscate a mobile phone and/or headphones that have been used without permission and hand it to the School Office. The School Office will record and parents will be notified via the Class Charts app. The pupil will expected to hand their phone and/or headphones into the School Office the following day. The number of days the pupil will be expected to leave their phone and/or headphones will be determined by the number of confiscations within a term:

- 1st offence Left at the School Office for 1 day
- 2nd offence Left with the School Office for 3 days
- 3rd offence Left with the School Office for 5 days

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. 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 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 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. 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 Academy 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 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 their permission and/or knowledge, with the intention of viewing parts of 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 Academy 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 whether occurring in school or outside of it.

2 The Academy takes a zero tolerance approach to online sexual harassment and it 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 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 reassured and offered appropriate support, regardless of how long it has taken for them to come forward, and kept safe.

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 consensual and non-consensual sharing of nude and semi-nude images and videos sexual images;

5.2 sharing of unwanted explicit content;

5.3 sexualised online bullying;

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

5.5 sexual exploitation, coercion or threats; and

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

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 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 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 or following a trend, 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 known, reliable and trustworthy 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 Policy.

6 The Head 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 Policy.