Highams Park Academy Trust

Policy and Procedure for Online Safety

Date of Review	SLMT Lead	Trustee Approval
30th September 2021	Tom Capewell	30th September 2021

Date of next review: October 2022

Circulated to staff:

Highams Park
Academy Trust

Contents

1. *Introduction* 3
2. *Policy Governance* 3
3. *Scope of the Policy* 4
4. *Roles and Responsibilities* 4
5. *Online safety Education and Training* 6
6. *Communication methods and devices* 7
7. *Unsuitable/inappropriate activities* 9
8. *Incident Management* 12

Appendix 1 – Student Acceptable Use Policy 15

Appendix 2 – Staff, Volunteer, Community User Acceptable Use Policy 19

Appendix 3 – Use of Images Consent Form 23

Appendix 4 – Statement on Sexting 24

Appendix 5 – Rules for the use of mobile devices by students 25

1. Introduction

The School Online Safety Policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

2. Policy Governance

This Online Safety Policy is overseen by the Designated Safeguarding Lead and another member of the Senior Leadership Team.

There are other key members of staff who contribute to the policy, including the Chief Operations Officer, Network Manager, Head of Department for Computer Science and Head of Digital Learning.

3. Scope of the Policy

There are considered to be 4 main areas of risk with regards to Online Safety (KCSIE 2021, paragraph 124):

- **content**: being exposed to illegal, inappropriate or harmful content
- **contact**: being subjected to harmful online interaction with other users, including peer-on-peer abuse
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams

We recognise that Online Safety is an integral part of Safeguarding. We are acutely aware that existing and emerging technologies provide additional ways in which safeguarding issues can develop. Many of these technologies are equally an essential part of learning, as they also provide means for students to develop their knowledge and build important competencies for later life.

The aspiration of our policy is a mixture of prevention through filtering and technical systems, combined with education in sensible and safe practices.

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

4. Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school with regards to Online Safety:

4.1. Trustees

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

4.2. Principal

The Principal is responsible for ensuring the safety (including Online Safety) of all members of the school community.
The Principal and members of the Senior Leadership and Management Team (SLMT) should be aware of the procedures to be followed in the event of a serious Online Safety issue.

4.3. Designated Safeguarding Lead

Must be aware of the potential for safeguarding issues that arise from online behaviour, such as:

4.3.1. Sharing personal data

4.3.2. Access to illegal/inappropriate materials
4.3.3. Inappropriate on-line contact with adults/strangers
4.3.4. Potential or actual incidents of grooming
4.3.5. Peer-on-peer abuse, including the sharing of indecent images
4.3.6. Online bullying

4.4. Online Safety Coordinator

4.4.1. Leads the Online Safety Committee, which is made up of the members of staff referenced in Section 2
4.4.2. Takes responsibility for Online Safety issues in liaison with the Designated Safeguarding Lead
4.4.3. Ensures that all staff are made aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
4.4.4. Arranges training and advice for staff through the school's CPDL coordinator
4.4.5. Oversees the Online Safety education of students
4.4.6. Logs incidents to inform future Online Safety developments
4.4.7. Reports to SLMT and to Trustees

4.5. Network Manager / ICT Technical staff

The Network Manager is responsible for ensuring (as far as is reasonable and possible):

4.5.1. That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
4.5.2. That the school meets the Online Safety technical requirements outlined in any statutory Online Safety guidance
4.5.3. That users may only access the school's networks through a properly enforced password protection policy
4.5.4. That the school adheres to GDPR concerning any aspect of network security or storing of personal information on school systems

4.6. All Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

4.6.1. They have an up-to-date awareness of the current Online Safety policy and practices
4.6.2. As far as is possible, they have an up to date awareness of Online Safety matters
4.6.3. They have read, understood and signed the school Staff Acceptable Use Policy (AUP) before being given access to school systems
4.6.4. They report any suspected misuse or problem to the Online Safety Coordinator or Designated Safeguarding Lead
4.6.5. They understand their responsibility to educate the students in their care, and to educate themselves, with reference to Online Safety and the changing nature of the online world

4.7. Students

4.7.1. Are responsible for using the school ICT systems and mobile technologies in accordance with the Student Acceptable Use Policy (AUP), which they will be required to sign before being given access to school systems
4.7.2. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

4.8. Parents/Carers

Parents and carers are responsible for endorsing (by signature) the Student Acceptable Use Policy (AUP).

5. Online safety Education and Training

5.1. Education – students

It is essential that all students receive Online Safety education and that this education, as far as possible, keeps pace with the changing nature of the online world.

5.1.1. Online Safety education is provided through Computer Science lessons, as well as through the Citizenship and Critical Minds programmes where appropriate. This covers both the use of ICT and new technologies in and outside of school, including students' responsibilities for managing these.
5.1.2. Key Online Safety messages are reinforced in assemblies and through the tutorial programme.
5.1.3. Students are taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
5.1.4. Students are made aware of the risks and dangers involved in the sharing of indecent images, including with their peers, and of how to report inappropriate activity.

5.2. Education & Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

5.2.1. Online Safety training will be made available to staff as and when necessary and not only through the Safeguarding training that staff undertake at the start of each academic year.
5.2.2. An audit of the Online Safety training needs of all staff will be carried out at the point of policy review. Some colleagues may identify Online Safety as a training need within the performance management process.
5.2.3. All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety and Acceptable Use Policies.

5.3. Education and Training – Trustees

It is desirable that Trustees receive Online Safety awareness training and essential that they understand their responsibilities. Online Safety training will be made available to Trustees on the Trustees' Development Day where appropriate.

6. Communication methods and devices

The following table shows the school's policy on the use of communication methods and devices.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table, along with other useful notes.

	Staff & other adults				Students			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons			X				X	
Use of mobile phones in social time	X					X		
Taking photos or videos on personal mobile phones or other camera devices		X					X	
Use of personal devices eg tablets / laptops	X						X	
Use of personal email addresses in school, or on school network	X				X			
Use of school email for personal emails	X				X			
Use of forums	X						X	
Use of instant messaging	X							X
Use of social networking sites for personal use				X				X
Use of social networking sites for school use			X					X
Use of blogs	X						X	

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to school		Remain switched off and out of sight during the school day (see Appendix 5).
Use of mobile phones in lessons	Staff should only use their phone during lessons for the purposes of teaching and/or learning and for emergencies.	Only in exceptional circumstances in order to carry out a task linked to their learning.
Use of mobile phones in social time		Remain switched off and out of sight during the school day, with the exception of Y11 students in the Youth Centre and 6th Form students in 6th Form study and social areas.
Taking photos on personal mobile phones or other camera devices	In exceptional circumstances this is permitted as long as the images / video are promptly transferred onto the system and deleted from the device.	In specific circumstances for the purposes of teaching and learning only.
Use of personal devices eg tablets, laptops, etc.		Allowed in the 6th Form during study and social time. Also in 6th Form lessons with staff permission. Always at students' own risk.
Use of personal email addresses in school, or on school network	Any e-mails sent to students must be sent from the member of staff's school e-mail address to the student's school e-mail address.	
Use of social networking sites for school use	Departments in school may use social networking to promote the work they are doing and will have a named member of staff responsible for this.	

7. Unsuitable/inappropriate activities

The school believes that some activities, many of which are referred to below, would be inappropriate in a school context. The table below is by no means an exhaustive list and the school reserves the right to take action against users who access or promote material that the school considers to be harmful, but which does not appear on the list below. The school also recognises that there are ways in which those activities that are listed as 'Acceptable at certain times' or 'Acceptable for nominated users' could be harmful if incorrectly used. Again, the school reserves the right to take action against users whom the school considers to have engaged inappropriately in these activities. The school network security, of course, restricts certain internet usage.

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions					
Accessing child sexual abuse images					X
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
Accessing adult material, pornography, or material that potentially breaches the Obscene Publications Act in the UK					X
Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					X
Promotion of racial or religious hatred					X
Threatening behaviour, including promotion of physical violence or mental harm					X
Promotion of any other information which may be offensive to other members of the school community, runs contrary to the ethos of the school, or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X
Creating or propagating computer viruses or other harmful files					X
Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X
On-line gaming (educational)		X			
On-line gaming (non-educational)		X	X		
On-line gambling				X	
Accessing the internet for personal or social use (e.g. online shopping, banking etc)		X			
File sharing e.g. music, films etc					X
Use of social networking sites		X	X		
Use of video broadcasting eg Youtube		X			
Using external data storage devices (e.g. USB) for holding sensitive data				X	

This table indicates when some of the activities above may be allowed:

	Circumstances when these may be allowed	
User Actions	**Staff & other adults**	**Students**
On-line gaming (educational)		When directed by a member of staff in lessons or under supervision in a school IT room at break/lunch.
On-line gaming (non educational)	Not acceptable	Under supervision in a school IT room at break/lunch.
Accessing the internet for personal or social use (e.g. online shopping, banking etc)	Before the start of the school day, after the end of the school day, or during a break or lunch.	Before the start of the school day, after the end of the school day, or during a break or lunch.
Use of social networking sites	For personal use - before the start of the school day, after the end of the school day, or during a break or lunch. For school-related activities – as appropriate and for those nominated users as specified above.	Not acceptable
Use of video broadcasting eg Youtube	For educational purposes only	For educational purposes only

8. Incident Management

Incidents (students):	Refer to teacher\tutor	Refer to Head of Department / Head of Year / other	Refer to Designated Safeguarding Lead (DSL)	Refer to Police	Refer to Network Manager	Inform parents / carers	Removal of network / internet access rights	Sanction according to severity of offence
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)			X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X						X	X
Unauthorised use of mobile phone/digital camera / other handheld device	X					X		X
Unauthorised use of social networking/ instant messaging/personal email	X					X		X
Unauthorised downloading or uploading of files					X		X	X
Allowing others to access school network by sharing username and passwords	X				X		X	X
Attempting to access or accessing the school network, using another student's account		X			X		X	X
Attempting to access or accessing the school network, using the account of a member of staff		X			X	X	X	X
Corrupting or destroying the data of other users		X			X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X

Incidents (students):	Refer to teacher\tutor	Refer to Head of Department / Head of Year / other	Refer to Designated Safeguarding Lead (DSL)	Refer to Police	Refer to Network Manager	Inform parents / carers	Removal of network / internet access rights	Sanction according to severity of offence
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X	X	X	X	X

Incidents (staff and community users):	Refer to SLMT	Refer to Police	Refer to Network Manager	Removal of network / internet access rights	Refer to Online Safety Coordinator	Sanction according to severity of offence
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	X	X	X	X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email					X	X
Unauthorised downloading or uploading of files	X	X	X		X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account			X		X	X
Careless use of personal data eg holding or transferring data in an insecure manner			X		X	X

Incidents (staff and community users):	Refer to SLMT	Refer to Police	Refer to Network Manager	Removal of network / internet access rights	Refer to Online Safety Coordinator	Sanction according to severity of offence
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X		X		X	X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	X		X		X	X
Actions which could compromise the staff member's professional standing	X		X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X				X	X
Using proxy sites or other means to subvert the school's filtering system	X		X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X	X
Deliberately breaching copyright or licensing regulations	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X

Appendix 1 – Student Acceptable Use Policy

Student Acceptable Use Policy

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to technology to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following I **WILL** and
I WILL NOT statements. If there's anything you're not sure of, ask your teacher.

I WILL:

- keep my username and password to myself at all times – I will not share it, or try to use any other person's username and password
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use my personal devices (mobile phones, etc.) in school if I have permission (see rules on mobile devices)
- follow the rules set out in this agreement, in the same way as if I were using school equipment, if I do use my own devices in school
- only use non-educational websites with permission and at the times that are allowed
- ask a member of staff if I am unsure about anything connected to my use of school IT equipment or the internet
- behave in the same way I would in class if my lesson is being conducted online, both in respect of my behaviour towards members of staff and towards other students

I WILL NOT:

- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- take or share images (pictures and videos) of anyone without their permission
- use the school IT systems for watching videos (eg YouTube), shopping online or other non-educational activities, unless I have permission of a member of staff to do so
- use the school IT systems for any illegal purpose
- try to use any websites or software that might allow me to bypass the filtering/security systems in place to prevent access to inappropriate materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email (this is due to the risk of the attachment containing viruses or other harmful programmes)
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings
- disclose or share personal information (including pictures and videos) about myself or others when online.
- arrange to meet people off-line that I have communicated with online, without my parents' express permission and knowledge

Highams Park
Academy Trust

Student Acceptable Use Policy Agreement Form

This form relates to the student Acceptable Use Policy (AUP), to which it is attached.

Students:

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, covered in this agreement, when I am out of school and where they involve my membership of the school community (examples, but by no means an exhaustive list, could include cyber-bullying, use of images or use of personal information).
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may (depending on the severity of the incident) include loss of access to the school network/internet, detentions, contact with parents, fixed-term exclusions and, in the event of illegal activities, involvement of the police.

I have read and understood the above and agree to follow this policy when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Firefly, the school website etc.

Parents/Carers:

Parents/Carers are required to sign this form below, alongside their child, to show their support of the school in this important aspect of our work.

Name of Student		
Tutor Group		
Signed (Student)		Date
Signed (Parent/Carer)		Date

Appendix 2 – Staff, Volunteer, Community User Acceptable Use Policy

Staff, Volunteer and Community User Acceptable Use Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's Online safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- When using the internet in my professional capacity or for school sanctioned personal use:
    - I will ensure that I have permission to use the original work of others in my own work.
    - Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Highams Park
Academy Trust

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the Staff, Volunteer and Community User Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police

I have read and understand the attached AUP and the Online Safety Policy. I agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 3 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Members of staff (or students with staff permission) sometimes record photographic or video evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons, under the supervision of a member of staff.

Images may also be used to celebrate success through their publication in school newsletters, on school displays, on the school website, school social media accounts and, occasionally, in the public media (both in print and online).

The school complies with the GDPR and requests parents' permission before taking digital / video images of members of the school. Parents are requested to sign the permission form attached to the Student Information Booklet to allow the school to take and use images of their children.

5. Photographs / videos I understand that during my child's time at Highams Park school, staff may take photographs/videos of school activities that involve my child. The photographs/videos may be used for: traditional school photographs of both individuals and groups; school displays; school publications; the school website and other school-based social media. I give permission for the use of photographs and videos as described above.	☐

Signature required at the bottom of the student information collection form

Appendix 4 – Statement on Sexting

Statement on Sexting

We use the following definition of sexting at Highams Park School:

"Images or videos generated
• by children under the age of 18, or
• of children under the age of 18
that are of a sexual nature or are indecent."

At Highams Park School we understand that sexting presents a risk to the safety of students within our school. We understand that this is something that presents a risk to students in our school outside of school hours and, potentially, within school as well. We also understand that many students have unlimited and unrestricted access to the internet via mobile technologies and therefore can bypass security settings that the school puts in place.

We make every effort to educate the students at Highams Park School about the dangers of sexting and the ways in which they can avoid placing themselves at risk. This is done through curriculum time in Computer Science, Citizenship, Critical Minds and delivered centrally through assemblies and tutor time.

Where an incident of sexting comes to the school's attention the advice to staff is as follows:

- If a device is involved, secure the device and switch it off. Do not show any images to, or share any images with, anyone else.
- Seek advice from the Designated Safeguarding Lead (DSL) or Deputy DSL via normal safeguarding procedures as soon as possible.
- The DSL or Deputy DSL will deal with the incident and refer to the police where necessary.

Due to the complexity of managing sexting incidents and the legal position of students and staff, further information and advice is made available to staff through the "Managing Sexting Information" document and the "Sexting Advice and Guidance booklet" which can be found in Student Services, with the Online Safety Coordinator or the DSL.

Appendix 5 – Rules for the use of mobile devices by students

Highams Park School
Rules for the use of mobile devices (including phones and headphones) – Years 7-11

At Highams Park School we understand that mobile phones and other devices form an essential part of modern life, but that there are appropriate times to use them and other times when it is inappropriate to do so.

Rules for mobile devices (including phones and headphones)

- Mobile devices **must not be seen or heard** at any point during the school day.
- Mobile devices **must not be used** at any point during the school day.
- Mobile devices **must be kept in inside pockets or bags** during the school day.
- The school day means from the moment you walk through the gate in the morning until you have left the building at the end of period 5 or period 6.

Exceptions to this rule

- If **a teacher specifically asks you** to use your mobile device for educational purposes.
- If you are in Year 11 then you may use your mobile device **in the Youth Centre** at break and lunch.

What happens if you break these rules?

- If your device is seen or heard **in the classroom** your device will be confiscated without warning.
- If your device is seen or heard **around school** your device will be confiscated without warning.
- At the end of the day your device will be returned to you by a senior member of staff after 3.30pm from Student Services.
- If your device is **confiscated more than once in any half-term,** then a parent will have to collect the device on your behalf.
- If there are **persistent problems with your mobile device use**, then you will lose break and lunchtimes and may have to hand over your device to a senior member of staff at the start of each school day.

Highams Park
Academy Trust

Highams Park School

Rules for the use of mobile devices (including phones and headphones) – 6th Form

At Highams Park School we all understand that mobile phones and other devices form an essential part of modern life, but that there are appropriate times to use them and other times when it is inappropriate to do so.

The general principle for 6th Form students is that we want to treat you like adults. You have a number of privileges concerning the use of mobile devices that are not available to younger students. This is because we trust you to do things properly. By sticking to these rules, that will be able to continue.

Rules for mobile devices (including phones and headphones)

- Mobile devices **must not be seen or heard** outside of specific 6th Form areas at any point during the school day.
- Mobile devices **must not be used** outside of specific 6th Form areas at any point during the school day.
- Mobile devices **must be kept in inside pockets or bags** during the school day.
- The school day means from the moment you walk through the gate in the morning until you have left the building at the end of period 5 or period 6.
- You may use your mobile device if **a teacher specifically asks you** to for educational purposes.

Specific 6th Form areas

- You may use your mobile device in the **6th Form building** (but not during lessons in classrooms) at any point during the school day.
- You may use your mobile device, for educational purposes or for listening to music, in the **6th Form study areas** at any point during the school day.

What happens if you break these rules?

- If your device is seen or heard **in the classroom** your device will be confiscated without warning.
- If your device is seen or heard **around school** your device will be confiscated without warning.
- At the end of the day your device will be returned to you by a senior member of staff after 3.30pm from the 6th Form Block.
- If your device is **confiscated more than once in any half-term,** then a parent will have to collect the device on your behalf.
- If there are **persistent problems with your mobile device use**, then you will lose break and lunchtimes and may have to hand over your device to a senior member of staff at the start of each school day.