ST JAMES
SCHOOLS

Acceptable Use Policy for Pupils

St James Schools

December 2021

Contents

Clause

Appendix

1 Aims

1.1 This is the acceptable use policy for pupils of St James Independent Schools (**School**) including the Preparatory and Senior Girls' School and the Senior Boys' School.

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 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; and

(d) cyberbullying and other forms of abuse.

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

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

1.2.5 to ensure that pupils use technology safely and securely and are 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 promote a whole school culture of safety, equality and protection.

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

2 Scope and application

2.1 This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

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

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

3 Regulatory framework

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

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Statutory framework for the Early Years Foundation Stage (DfE, September 2021);

3.1.3 Education and Skills Act 2008;

3.1.4 Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) and

3.1.5 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);

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

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020);

3.2.4 Advice and guidance: How can we stop prejudice-based bullying in schools? (Equality and Human Rights Commission);

3.2.5 Sexual violence and sexual harassment between children in schools and colleges (DfE, September 2021);

3.2.6 Searching, screening and confiscation: advice for schools (DfE, January 2018);

3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019); and

3.2.8 Relationships education, relationships and sex education and health education guidance (DfE, June 2019).

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

3.3.1 behaviour, rewards and school discipline policy;

3.3.2 anti-bullying policy;

3.3.3 e-safety policy;

3.3.4 expulsion and removal: review procedure;

3.3.5 safeguarding and child protection policy and procedures;

3.3.6 risk assessment policy for pupil welfare

3.3.7 relationships and sex education policy; and

3.3.8 School rules.

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

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

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

5 Definitions

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

5.1.1 References to the **Proprietor** are references to the Board of Trustees of the Independent Educational Association Limited.

5.1.2 References to the **Head** include the Head of the Preparatory School, the Headmistress of the Senior Girls' School and the Headmaster of the Senior Boys' School.

5.2 The School 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 mobile phones and smart technology;

5.2.4 wearable technology;

5.2.5 desktops, laptops, netbooks, tablets/phablets;

5.2.6 personal music players;

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

5.2.8 social networking, micro blogging and other interactive websites;

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

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

5.2.11 gaming sites;

5.2.12 virtual learning environments such as Firefly;

5.2.13 wearable technology e.g. Apple iWatch;

5.2.14 SMART boards;

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 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	Designated Safeguarding Lead and Bursar	As required, and at least annually

Task	Allocated to	When/frequency of review
Keeping the policy up to date and compliance with the law and best practice	Designated Safeguarding Lead	As required, and at least termly
Monitoring the use of technology across the School, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change	Designated Safeguarding Lead and Network Manager	As required, and at least termly
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	Designated Safeguarding Lead and Network Manager	As required, and at least half termly
Online safety	Designated Safeguarding Lead	As required, and at least termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Designated Safeguarding Lead	As required, and at least termly
Seeking input from interested groups (such as pupils, staff, parents) to consider improvements to the School's processes under the policy	Designated Safeguarding Lead/Head of IT Strategy	As required, and at least annually
Formal annual review	Proprietor	Annually

7 Safe use of technology

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

7.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the School's curriculum and many of its policies and procedures. 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.childnet.com/resources/smartie-the-penguin

7.3.4 https://www.childnet.com/resources/digiduck-stories

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

7.3.6 https://www.disrespectnobody.co.uk/

7.3.7 http://www.safetynetkids.org.uk/

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

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

7.3.10 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 School's e-safety policy for further information about the School's online safety strategy.

7.5 Please see Appendix 7 for details of the School's response to online challenges and hoaxes.

8 Internet and Office 365/electronic communication systems

8.1 The School provides internet access, intranet and social media and electronic communication system Office 365 accounts to pupils to support their academic progress and development. Pupils are given individual user names and passwords to access the School's internet, intranet and email system and these details must not be disclosed to any other person.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet and Office 365/electronic communication system. 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 School network without completion of the BYOD Agreement by both the pupil and a parent/guardian. The use of any device connected to the School's network will be logged and monitored by the DSL and the Network Manager.

8.4 For the protection of all pupils, their use of Office 365/electronic communication and of the internet will be monitored by the School. Pupils should remember that records of files and communications exist and hence can be traced, even after deletion from a device. This includes but is not limited to email messages, chat posts, images, audio files and documents. Pupils should not assume that files stored on servers or storage media are always private.

9 School rules

9.1 Pupils **must** comply with the following rules and principles:

9.1.1 access and security (Appendix 1);

9.1.2 communicating online or off line using devices, apps platforms and use of internet and Office 365 (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 6); and

9.1.6 harmful online hoaxes and challenges (Appendix 7).

9.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

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

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 immediately.

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

10.3 The School has adopted a zero tolerance approach to sexual violence and sexual harassment - it is never acceptable and it will not be tolerated. Incidents of sexual violence or sexual harassment will not be dismissed as merely “banter” or “just having a laugh” or “boys being boys” as this can lead to the creation of a culture of unacceptable behaviours and an unsafe environment for children.

10.4 Pupils must not therefore use their own or the School's technology to bully others at any time, whether during or outside of school hours. Bullying incidents involving the use of technology, including cyberbullying will be dealt with under the School's anti-bullying policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

10.5 Any reports of sexual violence or sexual harassment will be taken extremely seriously by the School and those who have been victim to such abuse will be supported and kept safe throughout. No pupil should ever be made to feel that they have created a problem or feel ashamed for reporting their concern. Pupils should be aware that teachers may not be able to provide an assurance of confidentially in relation to their concern as information may need to shared further (e.g. with the School's Designated Safeguarding Lead) to consider next steps. See Appendix 6 for further information.

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

10.7 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.

10.8 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.

10.9 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Network Manager and the Designated Safeguarding Lead who will record the matter centrally in the E-safety register.

11 Sanctions

11.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Proprietor has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour, rewards and discipline policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures; withdrawal of the right to access the School's internet and Office 365/electronic communication facilities. Any action taken will depend on the seriousness of the offence.

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

11.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

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

12 Training

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

12.1.1 understand what is expected of them by this policy;

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

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

12.2 This may include but is not limited to: written information on online safety, presentations at staff meetings and INSET dates including hands-on training session on practical aspects of online safety.

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

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

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

13.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Designated Safeguarding Lead who 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 School's policies that apply to the retention and destruction of records.

14.2 All serious incidents involving the use of technology will be logged centrally in the E-safety register by the Designated Safeguarding Lead.

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

15 Version control

Date of adoption of this policy	December 2021
Date of last review of this policy	December 2021
Date for next review of this policy	August 2022
Policy owner (SMT)	Designated Safeguarding Lead
Policy owner (Proprietor)	Board of Trustees

Appendix 1 Access and security

1 Access to the internet from the School's computers and network must be for educational purposes only. You must not use the School'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 School'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 School network without without completing a BYOD agreement. For security reasons, authorised devices must be connected to the BYOD network only. This allows the IT department to ensure that approved devices are separated out from the main network and the correct security policies are applied.

4 For pupils below Year 12 the use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

5 For pupils in Year 12 and above, the use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while pupils are on School premises or otherwise in the care of the School is discouraged, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

6 Passwords protect the School's network and systems. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.

7 You must not knowingly gain (or 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 a member of the IT support team.

8 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.

9 The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or a member of the IT support team.

10 The School 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.

11 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails/electronic communications. If you receive an email with an attachment, or other downloadable material, you must not open the attachment, click on the link or try to download the material. You must inform the classroom teacher or IT support immediately. This also includes gaining access to a website you would expect to be blocked due to its content.

12 You must not disable or uninstall any anti-virus software on the School's computers.

13 You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School) without the advance written authority of the Head.

14 The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is discouraged.

Appendix 2 Use of the internet and Office 365/electronic communication

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

Use of the internet

2 You must use the School's systems for educational purposes only and are not permitted to access interactive or networking websites or applications when using School computers or, if using personal laptops or other devices authorised by the BYOD Agreement, on School premises unless this is expressly permitted for educational purposes.

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, unless a teacher has given you permission to do so (for example to complete a UCAS application).

4 You must not connect any external storage device whatsoever onto the School's systems. This includes but is not limited to hard disk drives, USB storage ('thumb' drives or CDs/DVDs.

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 create, display, view, retrieve, download, copy or otherwise distribute or share any illegal, offensive 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, 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 enter into any contractual commitment, whether for yourself or on behalf of another (including the School) without advance written authority from the Head.

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

Use of Office 365/electronic communication services

10 You will be provided with your own Office 365 account for School purposes and must not access any personal web based email account such as Gmail, Yahoo or Hotmail or electronic communication devices, apps or platforms via the School's network.

11 Your School Office 365 account can be accessed from home by using your normal log-in details. The School will not forward messages received during the School holidays.

12 You must only use your School Office 365 account for communication with staff. This includes Outlook (for email) and Teams (for chat) as well as any communication via shared documents. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

13 Email/electronic communications (including other forms of online or cloud based communication) should be treated in the same way as any other forms of written communication. You should not include or ask to receive anything in an email 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 emails could be forwarded to or seen by someone you did not intend.

14 You must not send or search for any email message which contains illegal offensive 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, homophobic, any form of bullying, 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 system in this way is a serious breach of discipline and may constitute a criminal offence.

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

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

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

18 You must not read anyone else's emails 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, MP3 players and wearable technology.

2 Pupils below Year 12 who bring a mobile device onto School premises (with the exception of those authorised by a BYOD agreement or permission from the Deputy Head Pastoral) must hand the mobile device to the phone monitor for their class before the start of the School day and may pick up the mobile device from the phone monitor at the end of the School day. All mobile devices are kept in the School Office during the School day.

3 The School acknowledges that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G).

4 For pupils below Year 12 the use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

5 For pupils in Year 12 and above the use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while pupils are on School premises or otherwise in the care of the School is discouraged, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

6 The use of mobile phones by pupils below Year 12 during the School day should not be necessary. In emergencies, you may request to use the School telephone. If your parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.

7 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 School in writing. Such a breach will result in immediate disqualification.

8 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.

9 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 content will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's anti-bullying policy and behaviour, rewards and discipline policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's child protection and safeguarding policy and procedures).

10 Pupils must not use their mobile and smart technology to send misogynistic messages or messages which contain language relating to sexual violence or which could be interpreted as being harassment, whether of a sexual nature or otherwise. The School has adopted a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour and discipline policy and also as a safeguarding matter under the School's safeguarding and child protection policy and procedures.

11 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the School's behaviour, rewards and discipline policy on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Head.

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

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 is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

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

6.1 **"Sharing nudes and semi-nudes** means the 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 School 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 School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection

procedures (see the School's safeguarding and child protection policy and procedures).

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

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

7 Upskirting

7.1 Upskirting typically involves taking a picture under a person's clothing without their permission and / or knowledge, with the intention of viewing 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 School will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

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

Appendix 5 BYOD Agreement

Here is a copy of our current BYOD Agreement:

https://forms.office.com/r/jRkwsU5r28

St James Senior Girls' BYOD Agreement

By submitting this form, you agree to the following conditions of use:

Device Types:

For the purpose of these conditions, the word 'device' means any privately-owned, portable, wireless electronic equipment that can be used for educational purposes. Typically this would include laptops, net-books, tablets.

- screen-size must be greater than or equal to the 10.5" netbook size
- phones are NOT permitted

Guidelines:

1. I agree that use of devices in lessons and form periods is at the sole discretion of the teacher in charge at the time.
2. I agree to comply with the teacher's requests at all times regarding the use of the device during lessons and form periods.
3. I understand and agree that all network traffic is monitored and that I am solely and completely responsible for all usage undertaken with my login details.
4. I will never share my login details with anyone else.
5. I take full responsibility for my device at all times.
6. If not required at any point during the day, the device will remain about my person or in my locker which must be subsequently secured with a padlock or equivalent (will not be provided by the school).
7. I agree that St James Senior Girls' School is not responsible for the security of the device.
8. I agree that devices must be brought to school **fully-charged** and must run off **batteries** during the day.
9. For safety reasons, I agree not to attempt to charge the device during the day.
10. For safety reasons, I agree not to use devices in corridors or whilst pupils are walking between rooms.
11. I am responsible for taking care of the device, including any costs of repair, replacement or modifications needed to use the device at school. I have insurance covering the device for theft, damage and loss.

12. I agree that St James Senior Girls' School reserves the right for a member of staff, authorised by the Headmistress, to inspect any device if there is reason to believe that school policies or rules may have been violated or that any other misconduct may have occurred with the device.

13. I agree that any misconduct or violations of other policies or rules involving a personal device may result in the loss of use of the device and/or further action being taken.

14. I agree that any ringtones/reminders/chimes must be set to silent whilst in lessons.

15. I agree not to use the device to record, transmit or post photos, audio or video of any people on the school site without receiving the express permission of a teacher.

16. I agree to use of the wireless network only and will not attempt to physically connect the device to the network.

17. I understand that support will be offered by St James IT support department on a "best efforts" basis and only as time allows.

Appendix 6 Online sexual harassment

1 Online sexual harassment means "unwanted conduct of a sexual nature" occurring online.

2 The School takes a zero tolerance approach to online sexual harassment and it is never acceptable and it will not be tolerated. The School will treat incidences as a breach of discipline and will deal with them under the School's behaviour and discipline policy and also as a safeguarding matter under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

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, and kept safe.

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

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

5.1 consensual and non-consensual sharing of indecent images and videos, including nude and semi-nude images and videos and sexual images;

5.2 the sharing of abusive images and pornography to those who do not wish to receive such content;

5.3 sexualised online bullying;

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

5.5 the sending of misogynistic messages; and

5.6 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 School's safeguarding and child protection policy and procedures.

8 The Head and staff authorised by them have a statutory power to search pupils/property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device contains illegal or undesirable material relating to online sexual harassment. The school's search procedures can be found in the school behaviour and discipline policy.

Appendix 7 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 School becomes aware that harmful online challenges or online hoaxes are circulating between pupils, the School will handle this as a safeguarding matter under the School's child protection procedures (see the School's safeguarding policy and child protection policy and procedures).

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

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 School's behaviour and discipline policy.

6 The Head and staff authorised by them have a statutory power to search pupils / property on school premises. This includes content of mobile phones and other devices if there is reasonable suspicion that a device is being used to commit an offence or cause personal injury or damage to property. The school's search procedures can be found in the school behaviour and discipline policy.