ST GEORGE'S ACADEMY

ONLINE SAFETY POLICY

Name of Designated Safeguarding Lead: Mrs Jeanette Steward
Name of Deputy Safeguarding Officer: Mrs Claire Crawshaw

1. Introduction

1.1 St George's Academy is committed to providing outstanding educational opportunities to all our students. The safety and welfare of our students is of the utmost importance. We believe that by ensuring that all can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

1.2 The Academy is committed to promoting and safeguarding the welfare of all students and an effective online safety strategy is paramount to this.

1.3 This policy is to support schools and educational settings work towards a safer community.

2. Aims of this Policy

2.1 The aims of this policy are threefold:

- To protect the whole school community from illegal, inappropriate and harmful
- content or contact
- To educate the whole School community about their access to and use of technology
- To establish effective mechanisms to identify, intervene and escalate incidents where appropriate

3. What is Online Safety?

3.1 Also called E Safety (or e-safety), Online Safety or Internet Safety, these all mean the same thing. It is about risk and being aware of the possible threats that online activity can bring, and how to deal with them.

3.2 These risks are grouped into four categories:

- Conduct: children's behaviour that may put them at risk
- Content: access to inappropriate or unreliable content that may put children at risk
- Contact: interaction with unsuitable, unpleasant or dangerous people that may put children at risk
- Commercialism: children's use of platforms with hidden costs that may put them at risk

3.3 Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online world and thus their digital footprint.

3.4 The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks.

3.5 E-safety forms a fundamental part of our safeguarding and child protection measures.

4. Our Responsibility

4.1 Schools have a dual responsibility when it comes to e-safety: to ensure the school's online procedures keep children and young people safe, and to teach them about online safety, in and outside of school.

4.2 We should foster an open environment in which children and young people are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world.

4.3 Government guidance across the UK highlights the importance of safeguarding children and young people from harmful and inappropriate online material (Department for Education, 2020).

4.4 A whole school approach to online safety is vital to ensure staff, governors, volunteers and parents teach children about online safety, through a consistent approach. Ultimately, the aim is for students to be able to navigate the digital world safely.

5. Online Safety – Understanding the Risks and Dangers (Risks and Definitions)

5.1 We know that developing technology brings opportunities; but it also brings risks and dangers. Children could face the following unsafe communications when online.

5.2 Age inappropriate content and access to unsuitable video and internet games - access to illegal, harmful or inappropriate images or other content such as violent or pornographic materials. Access to inappropriate games. Use of filters and monitoring programme in school. Parental settings and filters in the home.

5.3 Unauthorised access to, loss of, and sharing of personal information, personal data / GDPR - be aware of use of cookies these can be shared and sold. The use of online data could be stolen or shared with other people. Data could be used against you to blackmail and bully. Data breaches must be reported.

5.4 Child Criminal Exploitation: County Lines and Cyber Crime - school recognise that criminal exploitation of children is a geographically widespread form of harm that can affect children both in a physical and virtual environment.

5.4.1 County Lines Criminal Activity: Drug Networks or gangs groom and exploit children and young people to carry drugs and money from urban areas to suburban and rural areas, market and seaside towns. Key to identifying potential involvement in county lines are missing episodes, when the victim may have been trafficked for the purpose of transporting drugs. St George's will consider whether a referral to the National Referral Mechanism (NRM) should be undertaken in order to safeguard that child and/or other children.

5.4.2 Cybercrime Involvement: Organised criminal groups or individuals exploit children and young people due to their computer skills and ability, in order to access networks/data for criminal and financial gain. There are a number of signs that may indicate a pupil is a victim or is vulnerable to being exploited which include:

- Missing from education
- Show signs of other types of abuse/aggression towards others
- Have low self-esteem, and feelings of isolation, street or fear
- Lack trust in adults and appear fearful of authorities
- Have poor concentration or excessively tired

- Become anti-social
- Display symptoms of substance dependence
- Excessive time online computer/gaming forums
- Social Isolation in school with peers
- High-functioning with an interest in computing

5.4.3 This is not an exhaustive list and the Academy are aware of other factors which may also impact on the child. Like with all other safeguarding concerns, if our children are in this situation, support will be provided through the school or partner agency.

5.5 Child Sexual Exploitation: Safeguarding Concerns and Internet Grooming - children need to be aware that online connections are not always positive relationships or always honest and true. Some online users have the intent to sexually abuse and the internet is a common tool in order to do so. Often a relationship is initiated online- then offline. The vulnerable are prayed on. Fake profiles are common with the intention being to trick or deceive. (Catfishing and grooming) This can have sinister purposes. Risks being blackmailing, sharing of sexual images – child pornography, extortion, drug using, alcohol abuse, self-harm, kidnap and murder.

5.6 Youth Produced Sexual Imagery (Sexting) - youth produced sexual imagery refers to 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. It is illegal to send, share, view and download 'nudes' or images of a sexual nature. There are many dangers to this. Risks associated with exploitation, blackmailing, and bullying.

5.6.1 Sexting in schools and colleges: Responding to incidents and safeguarding young people - any situations involving students and youth produced sexual imagery are taken seriously as potentially being indicative of a wider safeguarding or child protection concern or as being problematic sexual behaviour. The understanding of children and young people around the potential implications of taking and/or sharing youth produced sexual imagery is likely to be influenced by the age and ability of the children involved. In some cases children under 13 (and indeed older) may create youth produced sexual imagery as a result of age appropriate curiosity or risk-taking behaviour or simply due to naivety rather than any sexual intent. Children under the age of 10 may also be involved; the fact that they are below the age of criminal responsibility is not relevant to the seriousness with which safeguarding concerns are considered. The age at which children are becoming involved in this issue is lowering all the time and as professionals we should be mindful of this.

5.6.2 We follow the guidance and principles in the document, 'Sexting in Schools & Colleges: Responding to incidents and safeguarding young people.'

5.6.3 All incidents involving youth produced sexual imagery will be responded to in line with the school's safeguarding and child protection procedures. When an incident involving youth produced sexual imagery comes to the attention of the school community:

- The incident is referred to the DSL as soon as possible and recorded using the usual safeguarding recording system
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- Parents/carers should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm

- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately

5.7 Upskirting - typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Staff should always act in the best interest of the child and follow usual safeguarding procedures.

5.8 Radicalisation and Promotion of Terrorism - events could be live streamed, risk of inappropriate images. The Prevent Strategy is key. Schools in the UK should also follow the Prevent duty's statutory guidance regarding online safety and radicalisation (UK Home Office, 2019). Read more about radicalisation and the Prevent duty. Extremism and Radicalisation see Appendix 7 of our Child Protection and Safeguarding Children Policy.

5.8.1 Referral process - as part of the duty to protect young people from the messages of extremism, the school may refer any young person they are concerned about to the local Prevent team through the Channel process. The Channel referral form can be found through the LSCB website link above and should be returned to the email provided channel@lincs.pnn.police.uk Before doing this the school should contact prevent@lincs.pnn.police.uk or PREVENT@lincolnshire.gov.uk to seek advice and support to see if a Channel referral is appropriate. Where the school has serious concerns about the vulnerability of a young person in relation to extremist behaviour, then the school should make a call to the Police on 999.

5.8.2 Our school, like all others, is required to identify a Prevent Single Point of Contact (SPOC) will be the lead within the organisation for safeguarding in relation to protecting individuals from radicalisation and involvement in terrorism. This will normally be the Designated Safeguarding Lead. The SPOC for St George's Academy is Mrs J Steward. The responsibilities of the SPOC are described in Appendix 8.

5.8.3 IT policies - settings are expected to ensure that children are safe from online terrorist and extremist material, typically via appropriate levels of filtering. Settings can require pupils and staff to abide by acceptable user policies, which make clear that accessing such sites, is unacceptable. Using school equipment to send terrorist publications to others would be a criminal offence.

5.9 The Dark Web (or Deep Web) - accessed through dedicated software / specialised browsers. This is criminal, with the intent to cause harm and upset usually through drugs and weapons and uncensored content. An anonymity guise is used for users such as paedophiles and extremists to operate without being traced.
Important question – if a student was found to be on this – 'what were you looking for?'

5.10 Online Gambling/Gaming Disorder - can effect anyone at any age. Children can use and buy game items using a currency for betting which can be real cash. Loot boxes and clever ways are used to mislead vulnerable people. Poor gambling habits can affect mental health and future lifestyle choices. There are specialist devises / locks, which parents can enforce, and sites can be blocked. Never input bank details.

5.11 Online Fraud - identities can be stolen and information hacked. There are many online SCAMS, which aim to exploit vulnerable individuals. This is a criminal offence. Police and banks would need to be informed.

5.12 Illegal downloading of music or video files and file sharing, Plagiarism and copyright infringement - when a movie or song is produced and marketed, everyone involved in the process has monetary gains from the sale of that product. Therefore, that product is protected by copyright law so that it cannot be copied, reproduced or resold without their permission. If you did not pay for a song, movie or other media file that has a copyright, then downloading that file is a crime. Likewise, distributing a copyrighted media file, whether via electronic or non-electronic methods, without the express permission of the copyright holder is also illegal.

5.12.1 If I download music illegally, will I be prosecuted? If you download music illegally, you will be breaching the copyright in the work. However, although you will be sent warning letters and could be pursued for damages and an injunction for copyright infringement, the copyright holder usually sues the site which provides the illegal downloads for a remedy as they will be the one to have made money out of it. Those who run such sites are also guilty of a criminal offence under the Copyright, Designs and Patent Act 1988 and can face up to 10 years in jail and/or a fine.

5.13 An inability to evaluate the quality, accuracy and relevance of information on the internet -
Device Addiction - excessive use which may impact upon social and emotional development and learning. Could be an addiction to gaming, Apps, social media and can form a negative relationship with Technology. In 2018, Gaming disorders were recognised as a health issue.

5.13.1 Social Media and Mental Health - young people today are constantly visible through social media due to the time they spend on it. Popular social media apps are Facebook, Whatsapp, Tic tok and Snapchat. Issues related to this are low self-esteem, low body confidence and body dysmorphia, FOMO (Fear of Missing Out) and anxiety. This affects sleep patterns and can constantly disturb healthy routines.

5.13.2 Online Challenges - these can apply varying levels of risk. Video images could be shared, this could cause harm, bullying, distress and trolling. FOMO and a need to gain 'likes' are important to many children. A child may feel peer pressure to take part in this or may long to feel part of an online 'community'. This is not realistic.

5.13.3 Offline Vs Online Identity - social media influencers are un-realistic but children need to be educated to realise this. Someone who is influenced could curate a false identity or portray differently to reality to 'fit in'. See appendix A.

5.14 Cyber-Bullying - is ever increasing. This is exasperated by young people using social media '24/7'. Social media information can be used negatively against a person. Trolling is also common and some people do not feel they can block or stop this. Fake profiles and constant abusive messages sent from 'anonymous' bullies are usual practise. Snapshots taken of live streaming events for example can be watched by anyone at any time. Can be mass viewed. Many Apps such as Tic tok are live and uncensored. See appendix B.

5.15 Targeted Advertising and Pop-up Ads - an online profile is formed by sites and apps visited. Advertising can be specific and not always legitimate or appropriate to age. Aim to not click onto links/suggested ads.

5.16 Fake News and Hoax's - some information posted online could be untrue and aimed to mislead, trick or deceive. It is important that we educate not to 'share'. This may embarrass, promote bullying, trolling and affect online reputation. Aim to report any 'stories' to the online platform, be resilient and do not believe everything posted online.

5.17 Online Reputation - it is our duty to educate all young people and share awareness. It is vital to have a positive online reputation. This describes how you self-portray online and how others perceive you. The digital footprint is formed from all sites / apps, which are visited. More and more employers are looking at applicant's online reputation; this can affect future job prospects. Other risks are identity theft, grooming, and exploitation. It is important to have high security settings and manage own settings, also being mindful of posts and individual digital footprints.

5.17.1 Mobile phones are banned from the Academy Year 7-11. Misuse of videos taken in school and posted which puts the Academy into disrepute can lead to exclusion as well as cyber-bullying during the school day. Links with the police take place where required.

5.17.2 Use of mobile phones in Year 12/13 is at the discretion of subject teachers as there are benefits to their use within lessons on occasion. However, other use applies as above out of lessons and the supervision of a teacher. Sixth form students are ambassadors to the Academy and are expected to portray a positive role model to the younger years.

6. Safeguarding Remote Learners

6.1 Users refers to all staff, pupils, governors, volunteers and any other person working in or on behalf of the school, including outside agencies and Parents/Carers. Linked to Child Protection and Safeguarding Policy and Working from Home Compliance.

6.2 DFE Guidance for Covid-19. During current times there is blended, distance learning, virtual events and meetings which are remotely delivered. Academy Risk assessment is in place. Hazards are live streaming, video and audio could be misused. Professional setting and behaviour is important. Treat it like an extension of the classroom. Only use school accounts for emailing, never private accounts. Ensure the teacher has control of settings, camera, and microphones – moderate and control the chat facility for example. Parental consent must be attained for use. The Academy has clear expectations for staff and student behaviour. Not all our students have access to Technology, being mindful of including all users and not putting any at a disadvantage is important, arrangements in place for all students.

6.3 We all have a duty under numerous pieces of legislation to recognise threat, risk and harm and to take steps to safeguard. All employees should feel comfortable to intervene and make good professional decisions and escalate to the DSL for appropriate levels of decision making.

7. Roles and Responsibilities

7.1 The Governing Body -

7.1.1 The Governing Body as proprietor has overall responsibility for safeguarding arrangements within the school, including the school's approach to online safety and the use of technology within the school.

7.1.2 The Governing Body is required to ensure that all those with leadership and management responsibilities at the Academy actively promote the well-being of students. The adoption of this policy is part of the Governing Body's response to this duty.

7.1.3 The Link Governor for Safeguarding is the senior board level lead with leadership responsibility for the school's safeguarding arrangements, including the Academy online safety procedures, on behalf of the Governing Body.

7.1.4 The Governing Body will undertake an annual review of the Academy safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 7.1.2 above.

7.2 Principal and Senior Leadership and Management Team -

7.2.1 The Principal has overall executive responsibility for the safety and welfare of members of the Academy community.

7.2.2 The Designated Safeguarding Leads (DSL) are senior members of staff from the Senior Leadership Team (SLT) with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy.

7.2.3 The DSLs will work with the Head of ICT and the IT Manager (see below) in monitoring technology uses and practices across the Academy and assessing whether any improvements can be made to ensure the online safety and well-being of students.

7.2.4 The DSLs will regularly monitor the Technology Incident Log maintained by the IT Manager.

7.2.5 The DSL will regularly update other members of the SLT on the operation of the Academy safeguarding arrangements, including online safety practices.

7.3 IT Manager -

7.3.1 The IT Manager, together with their team, is responsible for the effective operation of the Academy's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the Academy network.

7.3.2 The IT Manager is responsible for ensuring that:

- The Academy's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack
- The user may only use the Academy's technology if they are properly authenticated and authorised
- The Academy has an effective filtering policy in place and that it is applied and updated on a regular basis
- The risks of students and staff circumventing the safeguards put in place by the Academy are minimised
- The use of the Academy's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation
- Monitoring software and systems are kept up to date to allow the ICT Team to monitor the use of email and the internet over the Academy's network and maintain logs of such usage

7.3.3 The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the Academy to safeguarding issues.

7.3.4 The IT Manager will report regularly to the SLT on the operation of the Academy's technology. If the IT Manager has concerns about the functionality, effectiveness, online safety suitability or use of technology within the Academy, he will escalate those concerns promptly to the appropriate members(s) of the Senior Leadership Team (SLT).

7.3.5 The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the DSL in accordance with the Academy's Child Protection & Safeguarding Policy and Procedures.

7.4 All Staff -

7.4.1 The Academy staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of Academy policies and of safe practice with the students.

7.4.2 Staff are expected to adhere, as far as applicable, to each of the policies referenced above.

7.4.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the Academy Safeguarding & Child Protection Policy.

7.5 Parents -

7.5.1 The role of parents in ensuring that students understand how to stay safe when using technology is crucial. The Academy expects parents to promote safe practice when using Technology and to:

- Support the Academy in the implementation of this policy and report any concerns in line with the Academy policies and procedures
- Talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour
- Encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support

7.5.2 If parents have any concerns or require any information about online safety, they should contact the DSL.

8. Education and Training

8.1 Students -

8.1.1 The safe use of Technology is integral to the Academy's ICT curriculum. Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices (see the Academy Curriculum Policy).

8.1.2 Technology is included in the educational programmes in the following ways:

- Children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- Children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
- Children are guided to recognise that a range of technology is used in places such as homes and academy and encouraged to select and use technology for particular purposes

8.1.3 The safe use of technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, Stay safe and MAD days and teaching students through Life Skills lessons / SOW:
Online Safety

- About the risks associated with using the technology and how to protect themselves and their peers from potential risks;
- To be critically aware of content they access online and guided to validate accuracy of information;
- How to recognise suspicious, bullying, radicalisation and extremist behaviour;
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- The consequences of negative online behaviour; and
- How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and sanctions for those who behave badly.

8.1.4 The Academy's Acceptable Use of ICT Policy for Students sets out the Academy rules about the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology.

8.1.5 Students are reminded of the importance of this policy on a regular basis.

8.2 Staff -

8.2.1 The Academy provides training on the safe use of technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

8.2.2 Induction training for new staff includes guidance on this policy as well as the Staff Code of Conduct, Email & Internet Policy and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including cyberbullying and radicalisation. (updates via emails, leaflets and training day events).

8.2.3 Staff also receive data protection guidance on induction and at regular intervals afterwards.

8.2.4 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the Academy's overarching approach to safeguarding.

8.3 Parents -

8.3.1 Information is available to parents via the website. Additionally, we offer the opportunity for parents to attend 'How to help' based sessions on online safety on an annual basis.

8.3.2 Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

9. Access to Academy Technology

9.1 The Academy provides internet and intranet access and an email system to students and staff as well as other Technology. Students and staff must comply with the respective Acceptable Use of Technology Policy when using Academy Technology. All such use is monitored by the IT Manager and his team.

9.2 Students and staff require individual user names and passwords to access the Academy internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.

9.3 No laptop, tablet or other mobile electronic device may be connected to the Academy network without the consent of the IT Manager. All devices connected to the Academy’s network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the Academy's network will be logged and monitored by the IT Support Department.

9.4 The Academy has a separate Wi-Fi connection available for use by visitors to the Academy. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

9.5 **Use of mobile electronic devices**

9.5.1 The Academy has appropriate filtering and monitoring systems in place to protect students using the Internet (including email text messaging and social media sites) when connected to the Academy's network. Mobile devices equipped with a mobile data subscription can, however, provide students with unlimited and unrestricted access to the internet. Since the Academy cannot put adequate protection for the students in place, students are not allowed to use their mobile devices to connect to the Internet including accessing email, text messages or social media sites when in the Academy's care. In certain circumstances, a student may be given permission to use their own mobile device to connect to the Internet using the Academy's network. Permission to do so must be sought and given in advance.

9.5.2 The Academy rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

9.5.3 The use of mobile electronic devices by staff is covered in the staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for Academy purposes except in an emergency.
9.5.4 The Academy's policies apply to the use of technology by staff and students whether on or off Academy premises and appropriate action will be taken where such use affects the welfare of other students or any member of the Academy community or where the culture or reputation of the School is put at risk.

9.6 Procedures for dealing with incidents of misuse

9.6.1 Staff, students and parents are required to report incidents of misuse or suspected misuse to the Academy in accordance with this policy and the Academy's safeguarding and disciplinary policies and procedures.

9.7 Misuse by students

9.7.1 Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the Academy's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

9.7.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the Academy's child protection procedures (see the Academy Safeguarding & Child Protection Policy).

9.8 Misuse by staff

9.8.1 Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the Academy Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.8.2 If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the Academy Safeguarding & Child Protection Policy.

9.9 Misuse by any user

9.9.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of ICT or the Principal.

9.9.2 The Academy reserves the right to withdraw access to the Academy's network by any user at any time and to report suspected illegal activity to the police.

9.9.3 If the Academy considers that any person is vulnerable to radicalisation the Academy will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

9.9.4 If any devices need to be seized and passed onto the police then the device(s) should be confiscated and the police should be called. The device should be turned off and locked away until the police are able to come and retrieve it. The Academy will act in accordance with the DfE guidance *Searching, screening and confiscation 2018.*

9.10 Monitoring and review

9.10.1 All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the IT Manager.

9.10.2 The DSL has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the Academy are maintained.

9.10.3 Consideration of the effectiveness of the Academy online safety procedures and the education of students about keeping safe online will be included in the Governors' annual review of safeguarding.

10.Key Contacts

10.1 There are useful resources about the safe use of technology available via various websites including:

- http://www.thinkuknow.co.uk/
- https://www.disrespectnobody.co.uk/
- http://www.saferinternet.org.uk/
- https://www.internetmatters.org/
- http://educateagainsthate.com/
- http://www.kidsmart.org.uk/
- http://www.safetynetkids.org.uk/
- http://www.safekids.com/
- http://parentinfo.org/
- DfE's Advice for head teachers and School staff on cyberbullying
- DfE's Advice for parents and carers on cyberbullying
- DfE's Advice on the use of social media for online radicalisation

10.2 St George’s Academy include within their Life Skills the resource below:

- Online Safety Resource Pack available via the Stay Safe Partnership website Stay Safe Partnership Website.

10.3 Statutory Guidance and Legislative Framework in relationship to Online Safety:

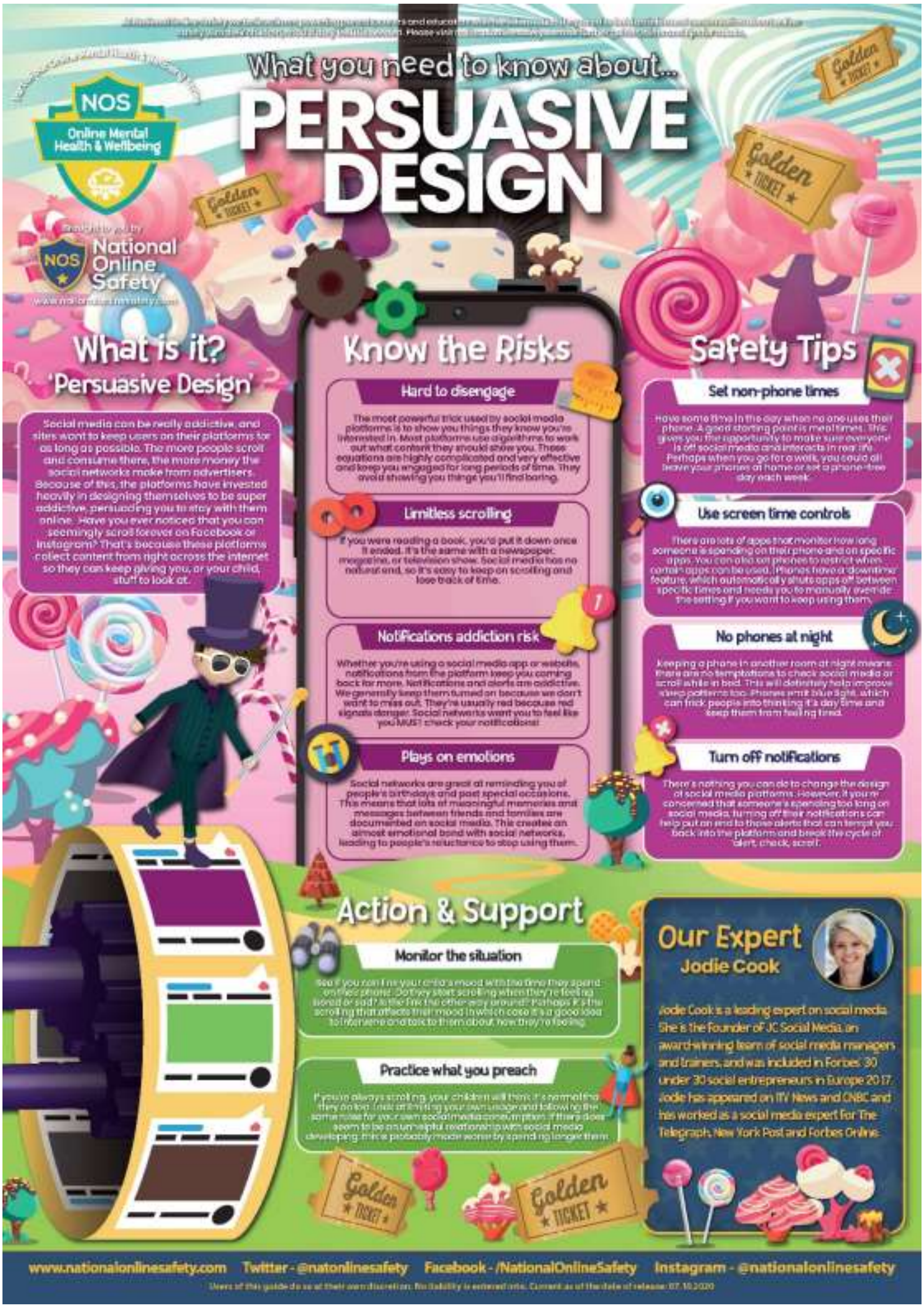
- Keeping Children Safe in Education 2020 (KCSIE)
- Relationships Education and Sex Education Guidance & Health Education 2019 (RSE)
- Education for a Connected World Framework 2019
- OFSTED Education Handbook

11.Other Related Academy Policies

11.1 Other related Academy policies that support this Online Safety policy include:

- Child Protection and Safeguarding Policy 2020
- Anti-Bullying Policy 2020
- Attendance Policy 2020
- Behaviour Policy 2020
- Special Educational Needs and Disability Policy 2020
- Data Protection Policy 2020
- ICT- Social Networking Policy 2019
- IT and Communication Systems Policy 2020
- Life Skills Policy 2019
- Staff Code of Conduct
- Staff Training and Professional Development Policy 2020
- Whistle Blowing Policy 2019

Appendix A – Parent Guide to Persuasive Design



[illegible]

What you need to know about...

PERSUASIVE DESIGN

What is it? 'Persuasive Design'

Social media can be really addictive, and sites want to keep users on their platforms for as long as possible. The more people scroll and consume there, the more money the social networks make from advertisers. Because of this, the platforms have invested heavily in designing themselves to be super addictive, persuading you to stay with them online. Have you ever noticed that you can seemingly scroll forever on Facebook or Instagram? That's because these platforms collect content from right across the internet so they can keep giving you, or your child, stuff to look at.

Know the Risks

Hard to disengage

The most powerful trick used by social media platforms is to show you things they know you're interested in. Most platforms use algorithms to work out what content they should show you. These equations are highly complicated and very effective and keep you engaged for long periods of time. They avoid showing you things you'll find boring.

Limitless scrolling

If you were reading a book, you'd put it down once it ended. It's the same with a newspaper, magazine, or television show. Social media has no natural end, so it's easy to keep on scrolling and lose track of time.

Notifications addiction risk

Whether you're using a social media app or website, notifications from the platform keep you coming back for more. Notifications and alerts are addictive. We generally keep them turned on because we don't want to miss out. They're usually red because red signals danger. Social networks want you to feel like you MUST check your notifications!

Plays on emotions

Social networks are great at reminding you of people's birthdays and past special occasions. This means that lots of meaningful memories and messages between friends and families are documented on social media. This creates an almost emotional bond with social networks, leading to people's reluctance to stop using them.

Safety Tips

Set non-phone times

Have some time in the day when no one uses their phone. A good starting point is meal times. This gives you the opportunity to make sure everyone is off social media and interacts in real life. Perhaps when you go for a walk, you could all leave your phones at home or set a phone-free day each week.

Use screen time controls

There are lots of apps that monitor how long someone is spending on their phone and on specific apps. You can also set phones to restrict when certain apps can be used. Phones have a 'downtime' feature, which automatically shuts apps off between specific times and needs you to manually override the setting if you want to keep using them.

No phones at night

Keeping a phone in another room at night means there are no temptations to check social media or scroll while in bed. This will definitely help improve sleep patterns too. Phones emit blue light, which can trick people into thinking it's day time and keep them from feeling tired.

Turn off notifications

There's nothing you can do to change the design of social media platforms. However, if you're concerned that someone's spending too long on social media, turning off their notifications can help put an end to those alerts that can tempt you back into the platform and break the cycle of alert, check, scroll.

Action & Support

Monitor the situation

See if you can link your child's mood with the time they spend on their phone. Do they start scrolling when they're feeling bored or sad? Is the link the other way around? Perhaps it's the scrolling that affects their mood in which case it's a good idea to intervene and talk to them about how they're feeling.

Practice what you preach

If you're always scrolling, your children will think it's normal that they do too. Look at limiting your own usage and following the same rules for your own social media consumption. If there does seem to be an unhelpful relationship with social media developing, this is probably made worse by spending longer them.

Our Expert

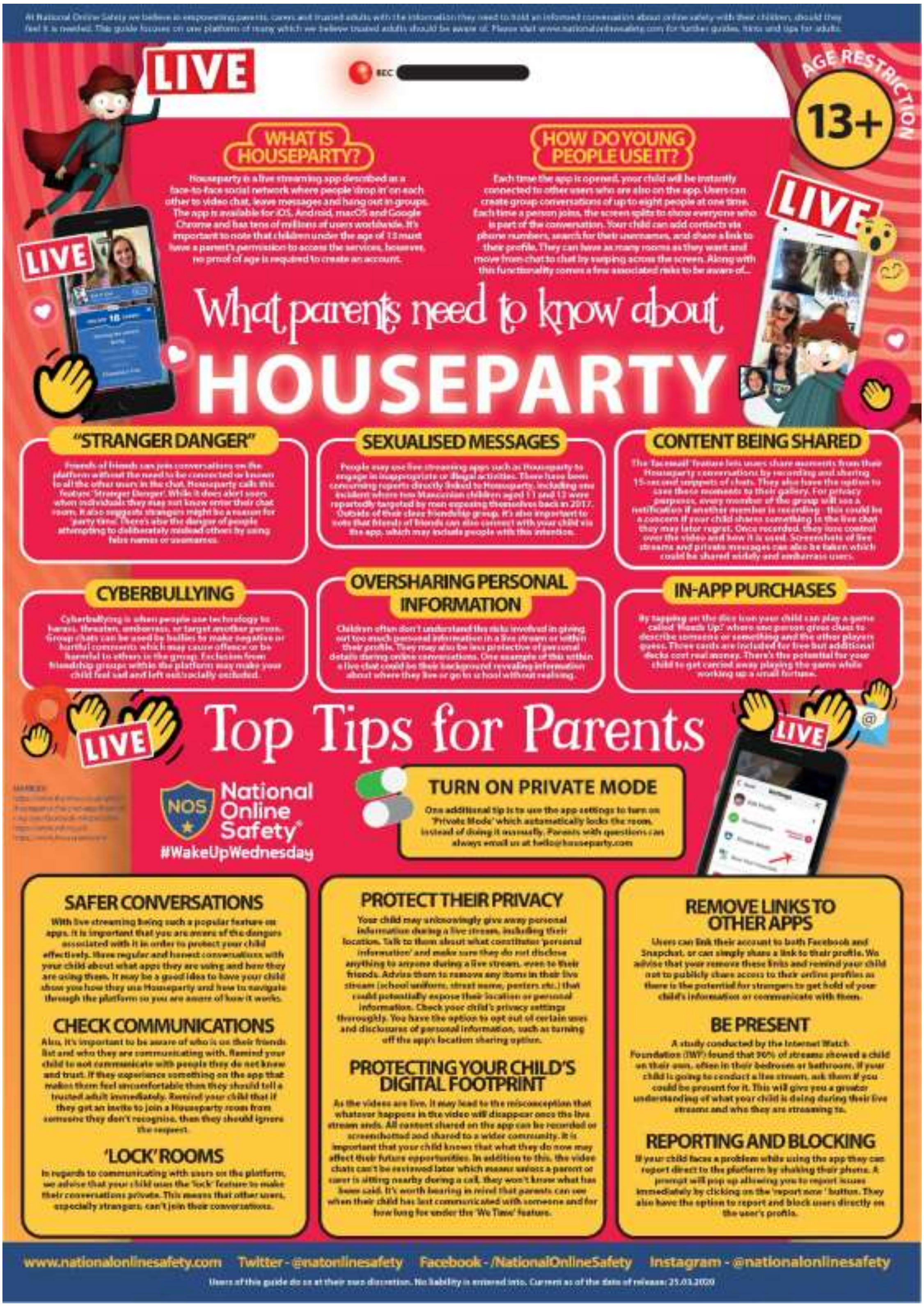
Jodie Cook

Jodie Cook is a leading expert on social media. She is the Founder of JC Social Media, an award-winning team of social media managers and trainers, and was included in Forbes 30 under 30 social entrepreneurs in Europe 2017. Jodie has appeared on ITV News and CNBC and has worked as a social media expert for The Telegraph, New York Post and Forbes Online.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 07.10.2020

Appendix B – Parent Guide to House Party


LIVE
REC
AGE RESTRICTION
13+
LIVE
LIVE
LIVE
LIVE

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

WHAT IS HOUSEPARTY?

Houseparty is a live streaming app described as a face-to-face social network where people 'drop in' on each other to video chat, leave messages and hang out in groups. The app is available for iOS, Android, macOS and Google Chrome and has tens of millions of users worldwide. It's important to note that children under the age of 13 must have a parent's permission to access the services, however, no proof of age is required to create an account.

HOW DO YOUNG PEOPLE USE IT?

Each time the app is opened, your child will be instantly connected to other users who are also on the app. Users can create group conversations of up to eight people at one time. Each time a person joins, the screen splits to show everyone who is part of the conversation. Your child can add contacts via phone numbers, search for their usernames, and share a link to their profile. They can have as many rooms as they want and move from chat to chat by swiping across the screen. Along with this functionality comes a few associated risks to be aware of...

What parents need to know about HOUSEPARTY

“STRANGER DANGER”

Friends of friends can join conversations on the platform without the need to be connected or known to all the other users in the chat. Houseparty calls this feature 'Stranger Danger'. While it does alert users when individuals they may not know enter their chat room, it also suggests strangers might be a reason for 'party time'. There's also the danger of people attempting to deliberately mislead others by using false names or usernames.

SEXUALISED MESSAGES

People may use live streaming apps such as Houseparty to engage in inappropriate or illegal activities. There have been concerning reports directly linked to Houseparty, including one incident where two Mancunian children aged 11 and 12 were reportedly targeted by men exposing themselves back in 2017. Outside of their close friendship group, it's also important to note that friends of friends can also connect with your child via the app, which may include people with this intention.

CONTENT BEING SHARED

The 'Facemail' feature lets users share moments from their Houseparty conversations by recording and sharing 15-second snippets of chats. They also have the option to save these moments to their gallery. For privacy purposes, every member of the group will see a notification if another member is recording - this could be a concern if your child shares something in the live chat they may later regret. Once recorded, they lose control over the video and how it is used. Screenshots of live streams and private messages can also be taken which could be shared widely and embarrass users.

CYBERBULLYING

Cyberbullying is when people use technology to harass, threaten, embarrass, or target another person. Group chats can be used by bullies to make negative or hurtful comments which may cause offence or be harmful to others in the group. Exclusion from friendship groups within the platform may make your child feel sad and left out/socially excluded.

OVERSHARING PERSONAL INFORMATION

Children often don't understand the risks involved in giving out too much personal information in a live stream or within their profile. They may also be less protective of personal details during online conversations. One example of this within a live chat could be their background revealing information about where they live or go to school without realising.

IN-APP PURCHASES

By tapping on the dice icon your child can play a game called 'Heads Up!' where one person gives clues to describe someone or something and the other players guess. Three cards are included for free but additional decks cost real money. There's the potential for your child to get carried away playing the game while working up a small fortune.

Top Tips for Parents

SOURCES:
[illegible]

National Online Safety
#WakeUpWednesday

TURN ON PRIVATE MODE

One additional tip is to use the app settings to turn on 'Private Mode' which automatically locks the room, instead of doing it manually. Parents with questions can always email us at hello@houseparty.com

SAFER CONVERSATIONS

With live streaming being such a popular feature on apps, it is important that you are aware of the dangers associated with it in order to protect your child effectively. Have regular and honest conversations with your child about what apps they are using and how they are using them. It may be a good idea to have your child show you how they use Houseparty and how to navigate through the platform so you are aware of how it works.

CHECK COMMUNICATIONS

Also, it's important to be aware of who is on their friends list and who they are communicating with. Remind your child to not communicate with people they do not know and trust. If they experience something on the app that makes them feel uncomfortable then they should tell a trusted adult immediately. Remind your child that if they get an invite to join a Houseparty room from someone they don't recognise, then they should ignore the request.

'LOCK' ROOMS

In regards to communicating with users on the platform, we advise that your child uses the 'lock' feature to make their conversations private. This means that other users, especially strangers, can't join their conversations.

PROTECT THEIR PRIVACY

Your child may unknowingly give away personal information during a live stream, including their location. Talk to them about what constitutes 'personal information' and make sure they do not disclose anything to anyone during a live stream, even to their friends. Advise them to remove any items in their live stream (school uniform, street name, posters etc.) that could potentially expose their location or personal information. Check your child's privacy settings thoroughly. You have the option to opt out of certain uses and disclosures of personal information, such as turning off the app's location sharing option.

PROTECTING YOUR CHILD'S DIGITAL FOOTPRINT

As the videos are live, it may lead to the misconception that whatever happens in the video will disappear once the live stream ends. All content shared on the app can be recorded or screenshotted and shared to a wider community. It is important that your child knows that what they do now may affect their future opportunities. In addition to this, the video chats can't be reviewed later which means unless a parent or carer is sitting nearby during a call, they won't know what has been said. It's worth bearing in mind that parents can see when their child has last communicated with someone and for how long for under the 'We Time' feature.

REMOVE LINKS TO OTHER APPS

Users can link their account to both Facebook and Snapchat, or can simply share a link to their profile. We advise that your remove these links and remind your child not to publicly share access to their online profiles as there is the potential for strangers to get hold of your child's information or communicate with them.

BE PRESENT

A study conducted by the Internet Watch Foundation (IWF) found that 90% of streams showed a child on their own, often in their bedroom or bathroom. If your child is going to conduct a live stream, ask them if you could be present for it. This will give you a greater understanding of what your child is doing during their live streams and who they are streaming to.

REPORTING AND BLOCKING

If your child faces a problem while using the app they can report direct to the platform by shaking their phone. A prompt will pop up allowing you to report issues immediately by clicking on the 'report now' button. They also have the option to report and block users directly on the user's profile.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 25.03.2020

Policy Developed by: Jeanette Steward, Vice Principal

Date Adopted:

Reviewing Committee: Student Support

Frequency of Review: 2 Years

Date last reviewed:

To be reviewed by:

Name ……………………………………………… Signature ………………………………………………

Committee: