FORTES FORTUNA ADJUVAT
Since 1929

St George's
PREPARATORY SCHOOL
Preparing Children For Life

Author – L Fidrmuc, R Morris, C Timothy, A Moon

Designated Online Safety Officer – L Fidrmuc

Agreed by Directors and Available to Staff– May 2022

To be Reviewed – Annually

Online Safety Policy

Associated Online Safety Policies
Policies and Procedures for the Education Department and Youth Service
Issued July 2016

Introduction

The internet and constantly evolving technology have changed the way that children interact with the world. While this can offer opportunities to learn and express their creativity, this technology also offers new risks such as:

- Exposure to inappropriate material (either accidentally or deliberately)
- Cyber bullying
- Exposure to online predators
- Sexting
- Revealing too much personal information
- Radicalisation

Learning to recognise warning signs will allow trusted adults to intervene where appropriate and to lessen the impact of potential negative experiences. It is vital for **ALL STAFF** to stay well informed about the issues relating to what children are experiencing using social networking, webcams, blogs, instant messaging etc.

A ‘joined up’ safeguarding approach

Online safety is not purely about technology. For example if a child types a concerning word into Google, the response would be no different than if they had written it in their maths book. Many of the issues arising in online safety are behavioural and will be managed in the same way as in any other area of school life. Therefore, this policy should be read in conjunction with the Child Protection Policy and other safeguarding policies. Furthermore, any escalation or response should be joined up with any other safeguarding escalation procedures.

A more realistic approach

Traditional E-Safety messages such as ‘don’t post personal information online’ (the ‘just say no’ approach) are now almost meaningless as the whole point of social media for many young people is to share personal information. Also the huge range of online applications now used means that locking information down via privacy settings is almost impossible.

A more realistic and pragmatic approach is to encourage a culture where children and young people feel able to share concerns with a trusted adult, and discuss online safety issues openly. They should be encouraged to consider the scope of the potential audience to whom they are posting, the context they are posting in and to take responsibility for any potential consequences. They should understand that nothing put online can ever truly be considered ‘private.’

St George’s Preparatory School’s Responsibilities

St George’s has a duty of care to assess and prevent possible harm to children and young people. In terms of online safety, St George’s has a duty to:

- Oversee and monitor the safe use of technology when children are in our care and take action immediately if there is a concern about wellbeing.
- Ensure that all staff receive appropriate online safety training that is relevant and regularly updated.
- Ensure there are mechanisms in place to support young people and staff facing online safety issues.
- Implement online safety policies and acceptable use policies, which are clear, understood and respected by all.
- Educate young people, parents and the school community to build knowledge, skills and capability in online safety.
- Monitor how the school is portrayed online by parents, children and staff and demonstrate how this is monitored.
- Not request a website to be unblocked or application installed unless a risk assessment has been completed.

Awareness for young people and parents

St George’s should ensure that all children in our care are aware of their responsibilities around appropriate use of technology both inside and outside of school.

This awareness should be delivered in lessons, assemblies, events, newsletters and through the development of a culture of online safeguarding.

St George’s should pro-actively engage parents and carers about online safety and related issues.

Conduct for Staff

Staff must:

- Act on and escalate all online safety issues promptly and escalate to the designated online safety individual in the school in accordance with the Child Protection and other Safeguarding policies.
- Sign an acceptable use agreement and adhere to the responsibilities set out therein.
- Only use their work email address to communicate with parents / children (not their personal email address)
- If working remotely from home: do not divulge passwords to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; use a designated room or space to work from; keep the device locked up and secure at all times.
- Use every appropriate opportunity to link online safety into the everyday curriculum.
- Only use encrypted USB sticks for personal data.
- Only use websites and web based applications with students when they have been risk assessed, and staff have read and reviewed the terms and conditions, and are satisfied that they do not pose an online safety or data protection risk.
- **Not** allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unattended when logged on.
- **Not** send friend requests to (or accept friend requests from) students on social media platforms. It is acknowledged that sometimes this is complicated due to relatives etc. however caution should always be exercised in respecting professional boundaries.

- **Not** attempt to compromise or bypass online safety measures for the sake of expedience or convenience.

Designated Online Safety Officer in School
St George's must have a member of staff with designated online safety responsibilities. It is important to bear in mind that this is primarily a safeguarding role, not an IT role, and this member of staff should receive appropriate child protection training and be provided with sufficient time and resources to deliver their function. This individual must also be of sufficient seniority to challenge other staff members if they are in breach of policy.

This individual will be responsible for:

- Ensuring that children are educated about online safety and related issues.
- Monitoring online activity of children.
- Escalating safeguarding concerns where appropriate within the school and to the Education Department and other agencies such as MASH where appropriate.
- Maintaining a log of online safety incidents in the School along with any follow up.
- Approving and risk assessing the use of any web based applications that staff wish to use.
- Reviewing school online safety and practice. It is recommended that the school uses the 360 degree safe tool www.360safe.org.uk

While this individual will be central, **all** members of staff have a responsibility to be alert to online safety risks and know how to escalate concerns appropriately. Safeguarding is everyone's responsibility.

Internet Filtering and blocking

Internet filtering
St George's has their internet content filtered. This will remove the majority of undesirable content but it is important to bear in mind that *no filtering system is infallible* and some unpleasant content will inevitably sometimes get through. This is particularly true of image searches, where some unpleasant images are tagged with innocuous words.
Therefore St George's will ensure there is sufficient supervision in place, and that the school engenders a culture where children feel they can approach a trusted member of staff if they have seen anything which worries them.
Please note that most 'apps' circumvent filtering so their use is kept to a minimum and the web versions are used where possible.
Both the WIFI and wired networks are filtered for the following:
You have a Cyberoam CR25iNG which is applying a web filter to block categorised websites such as:

Pornographic Material

Nudity

Adult Content

URL Translation Sites

Drug related sites

Crime and Suicide related sites

Gambling sites

Militancy and Extremist sites

Phishing and Fraud sites

Sites with violence

Weapons related sites

Specific Blocked URLs

Requesting a website to be blocked or unblocked

Website unblocking*.* *It is the responsibility of the requesting member of staff* to ensure that they do not make a request to unblock a website, until they have a) Established that it has a legitimate business or educational purpose b) Assessed the content of the site for suitability for the age and profile of the children who will be seeing it. They should then make an email request to the Designated Online Safety Officer.

Monitoring

St George's will monitor children's online behaviour in school.
Technical monitoring software provides an important opportunity to 'overhear' issues of concern, and intervene where appropriate to avoid a negative or tragic outcome.
St George's has an internal monitoring system to check on all online activity (WIFI and Wired).
Issues that will be monitored for include (but are not limited to):

- Self harm
- Eating disorders
- Bullying
- Pornography
- Radicalisation
- 18 rated games and films

'False positives' in monitoring

The nature of technical monitoring software is that there will be many 'false positives' (such as 'moby dick'). *However the school understands not to dismiss all of the flags on this basis,* as some will be genuine.
It is for the school (and the staff who know the child) to make a judgement in context, taking into account the age, profile and background of the child, when considering how to proceed with an online concern. If there are ongoing child protection meetings then any observations of online activity will be documented and integrated into this.

Managing systems

St George's systems management includes:

- Management and maintenance of different user profiles for web filtering to ensure all children are protected to an appropriate level.
- Monitoring the selection of web based services chosen by staff, checking they are risk assessed in terms of online safety and data protection - and challenging where appropriate.

- Conveying clear messages to discourage all from connecting to 3G and 4G networks and unsecured domestic Wi-Fi networks, when on school premises
- Strongly discouraging the use of unencrypted USB drives.
- Monitoring the school's online profiles and reputation, including on unofficial sites.
- Conducting regular testing to ensure blocked content is still inaccessible.

Web Histories

For children
For safeguarding reasons, it may occasionally be deemed necessary to look at the web history of a child. The search and the reasons for the report will be documented in the child's file, and the outcome of the report integrated within any other child protection procedures.

For staff
On some occasions it will be legitimate to carry out a web history search for a member of staff. This will be a formal request as part of a disciplinary procedure or similar.

Mobile devices
Mobile devices accessing the internet via the 3G or 4G networks are not subject to the same filtering and monitoring that the School systems are. This means that these devices could potentially give access to unsuitable content while on School grounds and under School supervision, not only to the owner of the device but also to their peers.
For this reason personally owned mobile devices must not be used whilst supervising children.

Social Media

Social media is recognised as a particular risk area for children. Unlike in recent years, where young people would be on one platform, young people use a wide variety of online platforms to share personal content. This can mean that any risk and issues are more complex.
Age restrictions. Under U.S. Law a child must be a minimum age of 13 to use a social media platform.

Below are the age restrictions for the most common sites:
13: Twitter, Facebook, Instagram, Pinterest, Google+, Tumblr, Reddit, Snapchat, Secret
14: LinkedIn
16: Whatsapp
17: Vine, Tinder
18: Path
18 (but 13 with parent's consent): YouTube, Keek, Foursquare, WeChat, Kik, Flickr

Staff and Community Use of Social Media
All staff should ensure that their personal social media profiles are locked down and not publicly viewable, for example which school they work at; bearing in mind that default privacy settings change regularly and that there is really no such thing as 'private post' on social media.
Staff should not 'friend' or accept friend requests from students on their personal social media profiles (even after they have left school, until they are 18).
If parents or members of the community post negative comments about the School, or staff or students in the School, DO NOT respond, but instead escalate to the Headteacher.

Common Online Safety Issues

Cyber-Bullying

Bullying is behaviour that is deliberate, repeated more than once and is designed to be hurtful. This type of behaviour can happen both on and offline (and often both), so it is crucial to consider all surrounding behaviour.

The impact of online bullying. While cyber-bullying can be an extension of face-to-face bullying, it differs in several significant ways: the invasion of home and personal space; the difficulty in controlling the scale and scope of electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target is often different to 'offline' bullying.

Policies and signposts for reporting. St George's has anti-bullying policies which articulate that participating in such activity will not be tolerated, and which provide clear guidance as to who a child should contact if they feel that they or someone else is being bullied.

Support for the target. The target of cyber-bullying may be in need of emotional support. Key principles here include: reassuring them that they have done the right thing by telling someone; recognising that it must have been difficult for them to deal with; and reiterating that no-one has a right to do that to them. Refer to any existing pastoral support/procedures for supporting those who have been bullied in the school, and refer them to helpful information and resources.

Advice for the target. It is important to advise the person being bullied not to retaliate or return the message. Replying to messages, particularly in anger, is probably just what the bully wants. By not replying, the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the evidence and take it to their parent or a member of staff. Advise the pupil to think about the information they have in the public domain and where they go online. Advising the child to change their contact details, such as their Instant Messenger identity or mobile phone number, can be an effective way of stopping unwanted contact. However, it is important to be aware that some children may not want to do this, and will see this as a last resort for both practical and social reasons.

Consider bystanders. In cyber-bullying, bystanders can easily become perpetrators – by passing on or showing to others images designed to humiliate, for example by 'liking' or commenting on a post. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the target.

Contain the incident. Some forms of cyber-bullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. It is challenging to contain this when the content may be spread across numerous sites and networks. The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it. If you know who the person responsible is, ensure that they understand why the material is hurtful and ask them to remove it. If this is unsuccessful, you may be able to contact the Internet Service Provider to remove the content.

Involve the wider community. St George's provides parents and carers with information about cyber-bullying policies, procedures and activities, and opportunities for becoming involved.

Self harm

In March 2016, a report by Parent Zone found that over half of 13 to 20 year-olds surveyed (51%) have seen someone talk about suicide online and 61% of young people have seen someone talk about hurting themselves online.

There is also a phenomenon where some young people set up new IDs online in order to send themselves bullying messages- a type of digital self harm.

If a young person is considering harming themselves, they may go online to search for methods. If monitoring software flags up a term relating to self harm, this must be responded to in line with Child Protection procedures as a matter of urgency.

Radicalisation

Definition. Paragraph 7 of the Prevent Duty (UK Government advice for Schools) defines extremism as: *'vocal opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces.'*

Statutory requirements in the UK. As a result of the Counter –Terrorism and Security Act 2015, specified authorities (including schools) in the UK have a duty to have 'due regard to the need to prevent people from being drawn into terrorism.' This duty includes technical monitoring for signs of radicalisation.

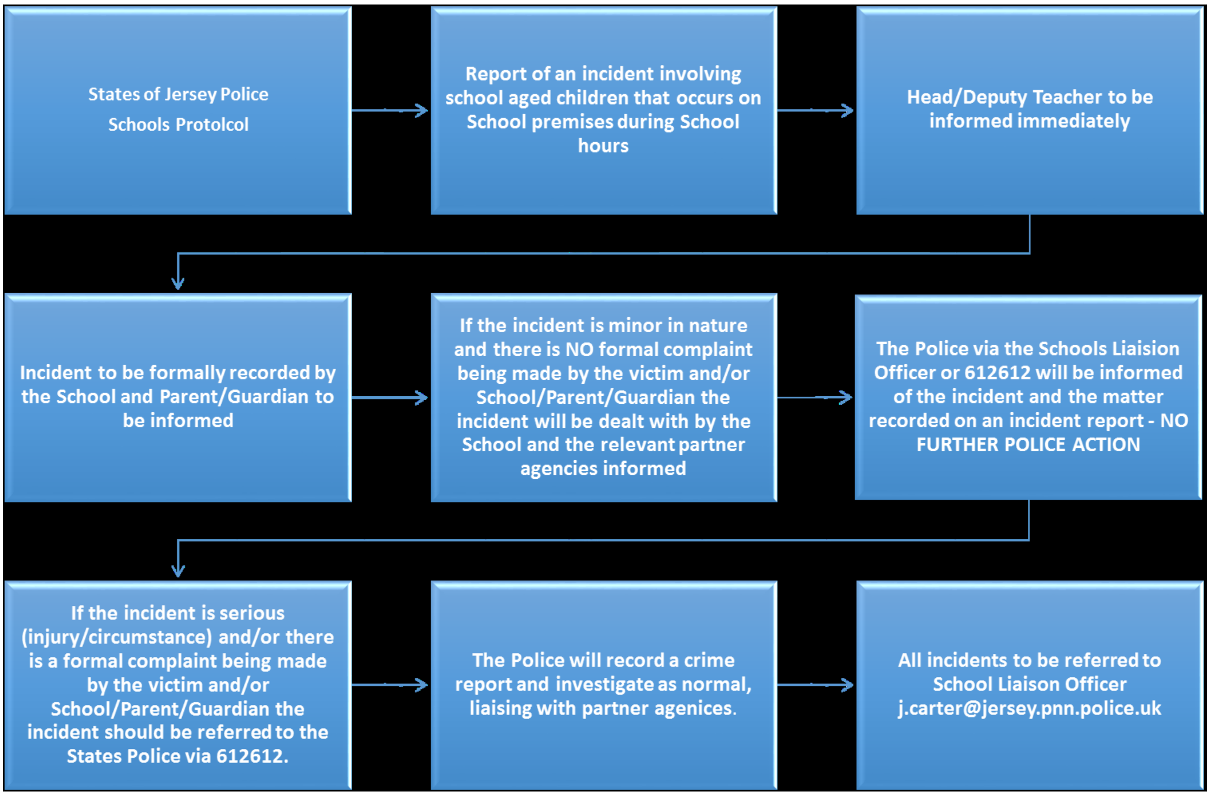
Does this affect Jersey? Extremist groups aim to target young people who are perhaps lonely, disenfranchised and want to feel part of a community. This can happen to any child of any background, in any geographical location who is using the internet, and Jersey is not immune.

Sexting

Definition. Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age.

The Law. Creating or sending an intimate photo of a minor is a criminal offence, so incidents need very careful management.

Response. If a device is involved, secure it and switch it off. Seek advice and report to your Designated Safeguarding Lead who should follow normal child protection procedures. Factors which would be taken into account in responding to sexting incidents include: the age of the person sending the photograph and the age of the person it was sent to; whether the individual was co-coerced into sending the image; to what extent the image has been shared online and whether the child is vulnerable and if there are existing concerns. The chart below is the official Jersey Police protocol for how to respond to a sexting incident and clarifies how and when the Police should become involved.



States of Jersey Police Schools Protolcol

Report of an incident involving school aged children that occurs on School premises during School hours

Head/Deputy Teacher to be informed immediately

Incident to be formally recorded by the School and Parent/Guardian to be informed

If the incident is minor in nature and there is NO formal complaint being made by the victim and/or School/Parent/Guardian the incident will be dealt with by the School and the relevant partner agencies informed

The Police via the Schools Liaision Officer or 612612 will be informed of the incident and the matter recorded on an incident report - NO FURTHER POLICE ACTION

If the incident is serious (injury/circumstance) and/or there is a formal complaint being made by the victim and/or School/Parent/Guardian the incident should be referred to the States Police via 612612.

The Police will record a crime report and investigate as normal, liaising with partner agenices.

All incidents to be referred to School Liaison Officer j.carter@jersey.pnn.police.uk

18 rated games and films

There is a growing phenomenon of children playing adult rated first person games such as Call of Duty or Grand Theft Auto. These games contain extreme violence, sexually explicit content, images of drug taking and other adult themes. In addition, children have access to adults from all over the world via the headset and multi-player options, which creates an added risk.

Research shows that parents often buy these games for their children, so working in partnership with parents and carers is crucial in tackling this issue.

What do I do if I have a concern about a young person's online activity?

A child's behaviour online does not exist in a vacuum. It is often an extension of their situation offline. Therefore it is vital to consider online behaviour in the context of the child's situation in general and any existing concerns.

Although IT expertise is helpful in investigating or obtaining a 'red flag' about a problem, do not forget that the underlying issue is not IT but safeguarding. Therefore, you should use the same criteria as for any other Safeguarding concern. Depending on your level of concern (and the background) it may be appropriate to make a MASH Enquiry via the Designated Safeguarding Lead (DSL).

There is a distinction between the kind of online activity which might result in a sanction (for example typing in swear words) and the type of activity (e.g. self harm) which calls for entirely different and considered approach and a high degree of judgement and sensitivity.

If you have any queries, speak to the DSL.

If you find illegal content

If you find illegal or potentially illegal content on the St George's network or a school-owned device, you must *immediately* close down the machine, secure the room or area and seek the advice of the Designated Safeguarding Lead (DSL). The DSL will then provide further advice and facilitate contact with the Police.

Do not forward, copy, print or save what you have found as this could potentially be a criminal act (i.e. making indecent images) and lead to a prosecution. The police will review the material and take appropriate action.

Images of Children (photos and video)

Parental consent to publish pictures. St. George's obtains parental consent to publish a picture of a child, whether on paper or online.

Consent forms. St George's has consent forms which record parental consent to publish pictures of their child. This form is completed at the beginning of the child's school career and can last for the duration of their time at the school. It does not have to be updated yearly however a parent has the right to change their mind and the school must record that decision. The consent form is split down into the following sections:

- Use on school website/ prospectus
- Printing in the Jersey Evening Post / local media
- Social media
- Webcam and Video
- In media with separate consent for identifying the child by name.

This information will be stored on a password protected central database.

Other legitimate use of images

Parents and carers can take pictures of their own children at St George's provided it is for their own personal use and not uploaded to social networking sites. Parents will be informed of this

during the welcome brief at school events. During larger events this message will be displayed in a visible location.
Staff / volunteers can take pictures to support educational aims, but must follow school policies regarding the sharing, distribution and publication of those images. The images should only be recorded on school owned devices, not personal devices. If it is necessary to use a personal digital camera, approval should be sought from the Designated Online Safety Officer or the Head Teacher. Pictures on personal digital cameras must be removed as soon as possible. Personal mobile phones or iPads must not be used to take pictures of children.
Care should be taken that students are appropriately dressed and are not participating in activities that might bring the school into disrepute.
Students must not take/use/share pictures of other students without permission.
Photographs published on the school website or elsewhere on behalf of the School will be selected carefully and appropriate consent sought.

Use and Storage of Photographs and Video Images Photographs taken as records of events or for educational purposes may be displayed around school on display boards and/or in evidence files and are then archived after use. Photographs are not exchanged with anyone outside school or held for private use. The staff are only permitted to take photographs and/or digital images of children in “school or educational provision settings” and may only use school approved and purchased cameras or recording equipment. The use of personal mobile phones to take digital images is not permitted.

Should the school learn about any inappropriate use of images involving children, the school will take immediate and proportional action including, if judged necessary by staff in consultation with the Head Master, recording and reporting any incident which could raise child protection concerns.

Data Protection and social media.

Care should be exercised when publishing pictures as for data protection reasons the data will be stored in a jurisdiction which is not protected by European Data Protection Laws.

If there is a dispute over consent

If one parent gives consent and the other does not, you should proceed as if no consent has been given. N.B. you must have legal parental responsibility to give consent.

Web based applications.

If you use photo or video streaming applications such as Skype, the School is sharing a child’s image with a third party. Parental consent must be sought before any such activity.

Please refer to the Data Protection Policy for related advice on this issu

St George's Preparatory School

Online Safety Policy

Appendices

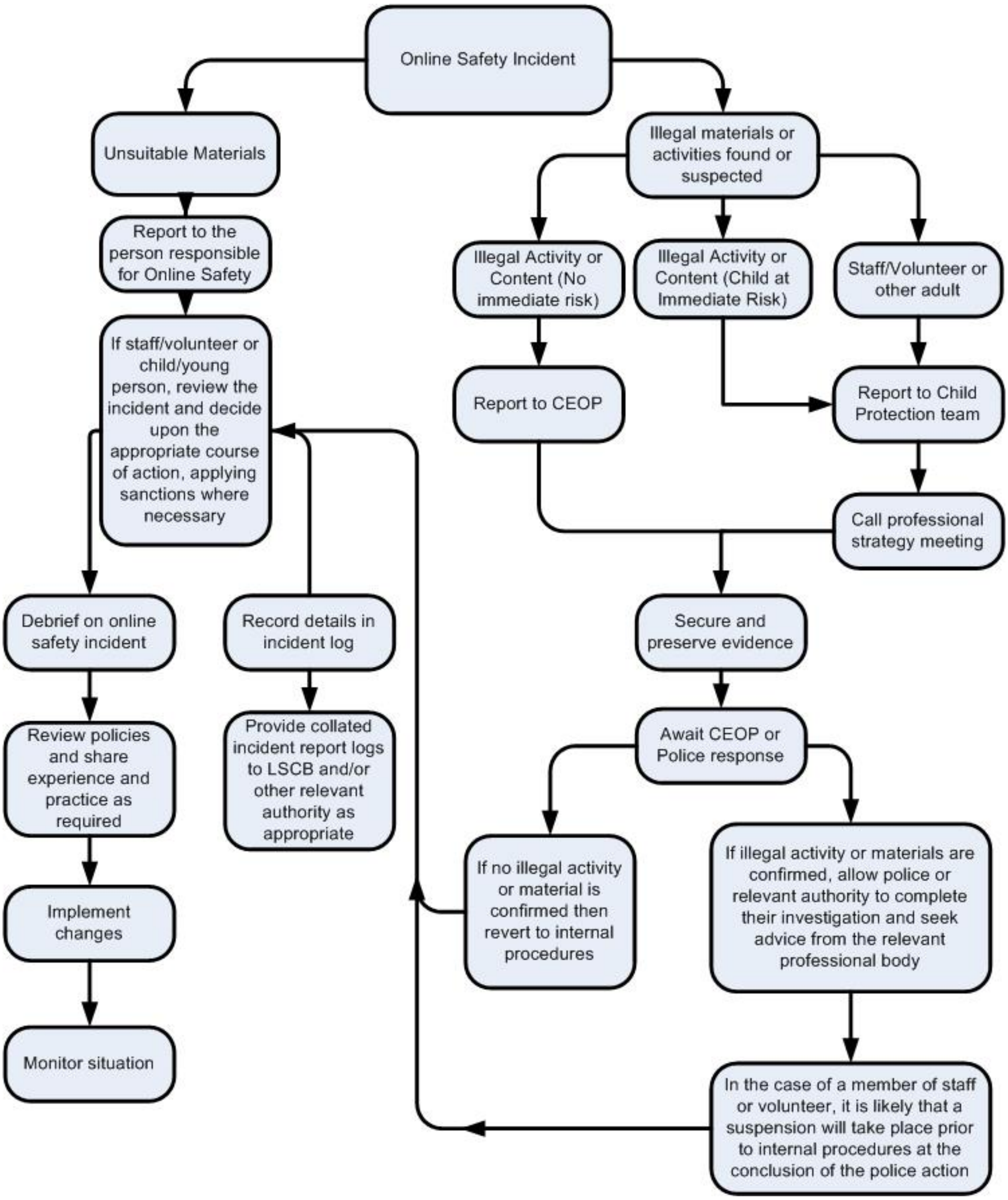
Appendix 1 – Responding to Incidents of Misuse

Appendix 2 - Incident Reporting Log

Appendix 3 – Acceptable Use Policy Agreements

(Young child/ Older Child/ Staff / Parent and Carer)

Appendix 1: Responding to incidents of misuse


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2 - Incident Reporting Log

Incident Details			Action Taken			
Date	Time	Incident	What?	By Whom?	Reported to DSL?	Signature

- If an incident is serious enough to report to the DSL. This form should be printed off and signed by the reporting member of staff once it is complete

St George’s Preparatory School

Pupil Acceptable Use Policy Agreement (Foundation / KS1/ Form III)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):………………………………………………

Signed (parent): …………………………………………..

Date:………………………..

St George's Preparatory School

Pupil Acceptable Use Policy Agreement
(Form IV- Form VI)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that St George's will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc)
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that St George's systems and devices are for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads.
- I will not use St George's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of an adult to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that St George's has a responsibility to maintain the security and reliability of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile devices / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand that mobile phones are not allowed in school.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to inappropriate materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person who sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites whilst at school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful.

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

- I understand that St. George's has the right to take action if I am involved in incidents of inappropriate behaviour. This includes when I am out of school. Examples include cyber-bullying, use of images or personal information.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

St George's Preparatory School

Pupil Acceptable Use Policy Agreement Form

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)

- I use my own devices in school (when allowed) eg gaming devices, USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of the school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil	
Class	
Signed	
Date	

Parent / Carer Countersignature

Signed	
Date	

St George's Preparatory School

Staff and Volunteer Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school when supervising children
- I will only communicate with parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities or the reputation of the school.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow the guidelines set out in the Online Safety Policy. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without prior consent from a member of the SLT.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred

outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Directors and in the event of illegal activities the involvement of the police.

St George’s Preparatory School

Staff and Volunteer Acceptable Use Agreement Form

This form relates to the Staff and Volunteer Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

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

Staff / Volunteer Name

Signed

Date

<u>St George's Preparatory School</u>

Parent / Carer Acceptable Use Agreement

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above pupil I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will read the Acceptable Use Agreement that my son / daughter has signed and ensure that he / she understands the content of the agreement.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed Date