States of Guernsey
Education Services

Policy Directive, Procedures and Guidelines

ONLINE SAFETY POLICY & GUIDANCE ON SEXTING IN SCHOOLS

Publication Date:	December 2019	Version Date:	2019.12.20
Review Date:	May 2022	Version Number:	V2.0
Contact:	Head of Inclusion and Services for Children and Schools		
✉:	educationsportandculture@gov.gg		
🖃:	Sir Charles Frossard House La Charroterie St Peter Port GY1 1FH		
☎:	+44 (0)1481 733000		
	www.gov.gg/education		

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the ConnectED Intranet is the controlled copy. As a controlled document, it should not be saved onto local or network drives but should be accessed from the ConnectED Intranet.

Summary of Changes[1] from Previous Versions

Version no/Date	Change	Comment	Section/ Page
V2.0 / December 2019	• Updated to new Data Protection (Bailiwick of Guernsey) Law 2017 • Links updated throughout document • Updated terminology from Cyber-bullying to Online bullying		9 /16
	Table started September 2019		

[1] Material changes only. Minor changes (such as to punctuation, grammar, etc.) will not be listed

Contents

1.0 Introduction

The internet and constantly evolving technology has changed the way that people 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)
- Online 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 learners are experiencing using social networking, webcams, blogs, instant messaging etc.

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.'

1.1. Policy Statement

This Online Safety Policy Directive is designed to safeguard and protect learners and staff. It sets out the key principles expected of all members of the school community with respect to the use of IT-based technologies.

Online safety is not purely about technology. For example if a child types a concerning word into Google, the response from the teacher 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. This policy should be read in conjunction with the Child Protection Policy and other safeguarding policies in school and alongside guidance from the Islands Safeguarding Children Partnership. Furthermore, any

escalation or response should be joined up with any other safeguarding escalation procedures.

Should there be an incident of online bullying, or other online safety incident covered by this policy directive, which may take place out of school, but is linked to membership of the school, the Headteacher can implement sanctions for inappropriate behaviour where this is reasonable. The school will deal with such incidents within this policy directive and with associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

1.2 Policy Objectives

Assist staff working with young people to:

- Work safely and responsibly with the Internet and other IT and digital Communication technologies
- Have clear structures in place to deal with online incidents
- Minimise the risks attached to the use of these technologies.

For learners, the policy directive sets out to:

- Provide opportunities for learners to acquire knowledge and understanding about the risks of Online Safety
- Provide opportunities for learners to be equipped with the knowledge and understanding and skills they need to build resilience and minimise the risks associated with the use of these technologies
- Provide opportunities for learners to understand when to report something to a parent or adult

1.3 Policy Application

This policy applies:

- Across all phases at all States of Guernsey educational establishments including commissioned services
- To all employee groups (i.e. responsibility for reporting incidents is not restricted to teaching practitioners, learners, parents/carers, partner agencies, volunteers, visitors, contractors and community users who have access to and users of school ICT systems, both in and out of school

Throughout this policy directive, Headteacher also refers to Principals and Heads of Service, school refers to any educational establishment, including commissioned services and Child Protection Officer refers to the establishment's lead officer with responsibility for Child Protection/Safeguarding.

In addition there is an expectation that other educational establishments e.g. Grant Aided Colleges will apply these policies within their provision of services.

1.4 Accountabilities

Headteachers are accountable for:

- Implementing this policy directive
- Ensuring the online safety of members of the school community
- Ensuring the reporting and recording of Online Safety incidents that affect the safety and well- being of learners in their care
- Ensuring that the Child Protection Officer and other relevant staff receive suitable training to enable them to carry out their safety roles and to train other colleagues, as relevant
- Ensuring that all staff are aware of the procedures that must be followed in the event of an online safety incident taking place (including online safety incidents involving staff)
- To ensure that the school website includes relevant information on online safety

With regard to online safety the Child Protection Officer (or Safeguarding Officer) is accountable for:

- Day to day responsibility for online safety issues, including reviewing and monitoring reports
- Establishing and reviewing the school's online safety procedures
- Providing regular and appropriate feedback to Headteacher / SLT on online safety incidents that affect the safety and well-being of learners in their care
- Ensuring online safety incidents are recorded in line with School behaviour policy or, if escalated, recorded through the MASH referral process
- Act as the contact for BOOST and use the BOOST platform to develop their own online safety professional expertise and lead / facilitate training for all staff

1.5 Responsibilities

All staff are responsible for compliance with this policy directive. Staff should act as good role models in their use of ICT, the internet and mobile technologies.

1.5.1 Schools' responsibilities

Schools have a duty of care to assess and prevent possible harm to children and young people. In terms of online safety, schools have a duty to:

- Oversee and monitor the safe use of technology when learners are in their care and take action immediately if they are concerned 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 agreements, which are clear, understood and respected by all. Links to acceptable use agreement templates are in section 1.6
- Educate young people, parents and the school community to build knowledge, skills and capability in online safety
- Not request a website to be unblocked or application installed unless an assessment risk and benefits has been completed

1.5.2 Child Protection Officer

With regard to online safety this individual will be responsible for:

- Ensuring that children are educated about online safety and related issues
- Escalating safeguarding concerns where appropriate, within the school, to Education Services and to other agencies such as MASH where appropriate
- Maintain a log of online safety incidents along with any follow up in line with the School behaviour recording processes
- Reviewing school online safety and practice. It is recommended that the school uses the 360 degree safe tool www.360safe.org.uk to do this
- 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
- Undertaking training and actively monitoring reports of online activity via the provided filtering system. Access to this is facilitated through the service desk
- Ensure that different user profiles for web filtering are managed and maintained to ensure all children are protected to an appropriate level

1.5.3 Teaching and Support Staff are responsible for:

Ensuring that they have an up to date awareness of online safety matters and of the current school online safety procedures and practices it is essential that all staff understand their responsibilities, as outlined in this policy:

- Reading, understanding and applying the States of Guernsey Staff Acceptable Use Directive
- Reporting any suspected misuse or problem to the Child Protection Officer or Headteacher
- Ensuring that digital communications with learners take place within clear and explicit professional boundaries and be transparent and open to scrutiny

- Online safety education is effectively embedded in all aspects of the curriculum and other school activities
- Ensure learners understand and follow the school Online Safety procedures and Acceptable Use Agreement
- Supervise and monitor ICT activity in lessons, extra-curricular and extended school activities
- Understand the online safety issues related to the use of mobile technologies and monitor their use
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Staff must:

- Act on online safety issues and escalate to the Child Protection Officer in the school in accordance with the School behaviour, Child Protection and other Safeguarding policies
- Only use work email address to communicate with children (not personal email)
- If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; keep the device secure at all times
- Use every appropriate opportunity to link online safety into the everyday curriculum.
- Only use encrypted USB sticks for personal data
- **Not** allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unlocked when unattended
- **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

1.5.4 Learners

Schools should ensure that all children in their 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.

Schools should pro-actively engage parents and carers about online safety and related issues.

All teachers also have a responsibility to ensure that learners understand their responsibilities as listed:

- Learners adopt the school ICT systems in accordance with the Learner Acceptable Use Agreement
- Learners need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Learners should be made aware of and understand school procedures and policies on the use of devices
- They should also know and understand school policies on the taking/use of images and on online bullying
- Learners should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety procedures covers their actions out of school, if related to their membership of the school and it affects the safety and well-being of another pupil/student

1.5.5 Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is allowed)

1.5.6 Community Users

Community Users who access school ICT systems / website / Learning Platforms should be made aware of the Community User Acceptable Use Agreement before being provided with access to the school systems.

1.6 Associated Documents

The following links are available to States of Guernsey staff:

Data and Information Management Policy on ConnectED

Data Protection

States of Guernsey Acceptable Use Directive

Positive Mental Health and Wellbeing in Schools

The following links are publically available:

Student Pupil Acceptable Use Agreement Template (Younger)

Student Pupil Acceptable Use Agreement Template (Older)

Community Acceptable Use Agreement Template

2.0 Areas of Risk

The main areas of risk for schools can be summarised as follows:

	Commercial	Aggressive	Sexual	Values
CONTENT Child as **Recipient**	Adverts Spam Sponsorship Personal info	Violent and hateful content	Pornographic unwelcome sexual content	Bias Racist Misleading info or advice
CONTACT Child as **Participant**	Tracking Harvesting Personal info	Being bullied harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
CONDUCT Child as **Actor**	Illegal downloads Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

Original 3 C's Classification by EU Kids Online project

3.0 Online Safety and Child Protection

All staff should be aware of the potential for serious child protection issues that may arise from the above categories of risk, which may also include:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying

4.0 Online Safety Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

BOOST provides information, advice and guidance on incorporating online safety into the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned and progressive online safety programme should be provided as part of computing, PSHCE, and the wider curriculum; this will cover both the use of ICT and digital technologies in school and outside school. The programme should be regularly reviewed and updated in the light of technological changes and reported incidents

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities
- Learners should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Learners should be helped to understand the need for the Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues, developing criticality and helping them to understand how they can influence and participate in decision-making
- Expectations for Acceptable Use should be clearly communicated and may include posters, splash screens on school devices, newsletters, school diaries and reinforced in lessons where technology is used
- Opportunity should be taken to support positive mental health and wellbeing messages with regard to the benefits and risks of technology including the use of social media

5.0 Digital, Photographic and Video Images

Education Services staff can view the Policy Directive 'Use of Digital Images of Children and Young People' and the appropriate consent forms via ConnectED: Data Protection and Information Management

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.

6.0 Internet Filtering and Blocking

6.1 Internet filtering

States Schools have their internet content filtered centrally. 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 you need to ensure there is sufficient supervision in place, and that your school engenders a culture where children feel they can approach a trusted member of staff if they have seen anything which worries them.

Staff accounts have much less filtering applied than student accounts. Again, you can apply for sites to be unblocked to staff accounts via the Service Desk (requests will need to be approved by a member of the School's senior management team)
Please note that 'apps' may circumvent the central monitoring and filtering so keep their use to a minimum and use the web versions where possible.

6.2 Requesting a website to be blocked or unblocked or making a change request on the Helpdesk

Website unblocking. It is the responsibility of the requesting school to ensure that they do not make a Service Desk request to unblock a website, until they have a) Established that it has a legitimate business or educational purpose b) Impact assessed the content of the site for suitability for the age and profile of the children who will be seeing it. This rationale and risk assessment should be documented and retained within the school and periodically reviewed. If you request for a site to be blocked, the school should continue to check periodically that the content is still inaccessible.

Change requests. If your school wants to make a request to install an application or change a configuration, or any other 'change' to the default curriculum network, this must be requested via the Service Desk. Again, schools should take responsibility for impact assessing the consequences of any such change and of any online safety or data protection implications, *before* making such an application.

6.3 Monitoring

It is the responsibility of schools to monitor young people's online behaviour in school (and to be vigilant to their online behaviour outside of school where it affects their safety or the safety of others).
Technical monitoring software provides an important opportunity to 'overhear' issues of concern, and intervene where appropriate to avoid a negative or tragic outcome.
The Child Protection Officer is responsible for monitoring these reports, and should ensure that the task is delegated in their absence. The reports for States schools are available through the webfilter and access to this can be requested through the GILE service desk. Reports however will provide only basic flags about searches.

6.3.1 'False positives' in monitoring – don't be put off

The nature of technical monitoring software is that there will be many 'false positives' (such as 'moby dick'). However it is very important that you do not 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 should be documented and integrated into this.

6.4 Web histories and when to use them

For children/learners

For safeguarding reasons, it may occasionally be deemed necessary to look at the web history of a learner. You can raise this request as a Service Desk request - but do not name the learner in the request please ask for a call back. The search and the reasons for the report should be documented in the learner'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. All requests should be from the Headteacher to the Director of Education/HRBP who will request a web search on your behalf. Please do not raise this kind of request via a Service Desk request.

7.0 Mobile Technologies

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 you may decide that personally owned mobile devices must not be used in school at all, or only used at lunchtimes.

If your school allows children to bring mobile devices to school you must have an in school policy in place governing their safe and responsible use. There should also be a signed agreement with students and parents as to how the device should and shouldn't be used.

The table below sets out the current configuration of devices used in Schools.

	GILE Devices		Personal Devices		
	School owned for use by multiple users	Authorised device*	Pupil/Learner owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	[1]	[1]	[1]
Full network access	Yes – laptops No – tablets/ Chromebooks	No	no	no	No
Internet only	Yes	Yes	yes	yes	Yes
No network access		yes	Yes	yes	Yes

* Authorised device – purchased by the learner / family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[1] These devices are allowed to join the BYOD/Visitor wireless network however internet access is dependent on authentication

In addition to this policy there aspects that the school may wish to consider and be included in their technology procedures and Acceptable Use Agreements:

School owned / provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times / places / in school / out of school
- If personal use is allowed
- Levels of access to networks / internet (as above)
- Management of devices / installation of apps / changing of settings / monitoring
- Access to cloud services
- Taking / storage / use of images
- Exit processes – what happens to devices / software / apps / stored data if user leaves the school
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in school (learners / visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- The right to take, examine and search users devices in the case of misuse
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes

8.0 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. The Data Protection (Bailiwick of Guernsey) Law 2017 states that children 13 and over are able to give consent to the use of information society service (ie social media). Bear this in mind when asking children to use social media as part of their learning. 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

8.1 Staff and Community Use of Social Media

Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All staff should consider security settings on their personal Social media profiles bearing in mind that default privacy settings change regularly and that there is really is no such thing as 'private post' on social media.

Staff should not 'friend' or accept friend requests from students on their personal social media profile, it is acknowledged that sometimes this is complicated due to relatives etc. however caution should always be exercised in respecting professional boundaries.

If parents or members of the community post negative comments about the school or staff/students in the school, DO NOT respond but instead escalate to the Headteacher who should seek advice from the Director of Communications (Office *of the* Committee *for* Education, Sport & Culture)

States of Guernsey guidance on the use of social media is available for staff on the Bridge: Communication Manual: Social Media Guidelines

9.0 Data Protection

Personal data must be processed in accordance with the Data Protection (Bailiwick of Guernsey) Law 2017.
Further information regarding Education Services' staff responsibilities with regards to data protection is available on ConnectED: Data Protection

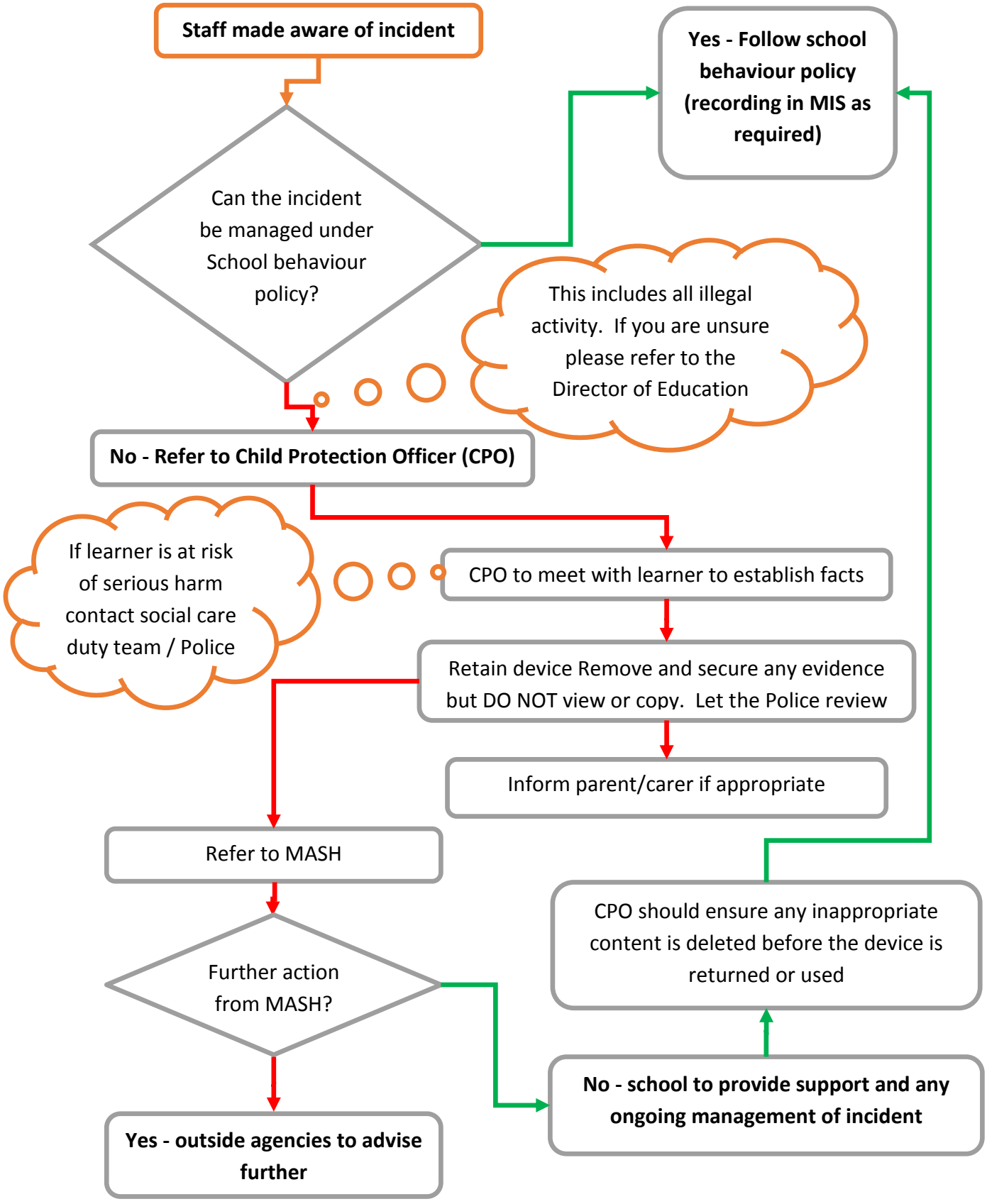
10.0 Responding to Incidents of Misuse

It is expected that all members of the school community will be responsible users of ICT, who understand and follow this policy directive. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse, this may or may not be illegal.

Examples of Illegal activity	Examples of non-illegal activity
• Child sexual abuse images • Material which potentially breaches the Obscene Publications (Bailiwick of Guernsey) Law 1985 • Criminally racist material • Material drawing people into radicalisation / terrorism • Other criminal conduct, activity or materials • Criminally threatening behaviour	• Using another person's username and password • Accessing websites which are against school policy e.g. games • Using a mobile phone to take unauthorised video during a lesson • Using the technology to upset or bully

The process outlined below should be followed. Where any apparent or actual misuse appears to involve illegal activity incidents must be referred to MASH, if you are unsure please contact the Director of Education or the Police.
Where the activity is not illegal and incidents must be recorded and escalated in line with the school's behaviour policy.

10.1 Online Safety Incident Process



11.0 Related Links

South West Grid for Learning: https://swgfl.org.uk/online-safety/
UK Safer Internet Centre: http://www.saferinternet.org.uk/
Digital Ace Guernsey: https://www.digitalacegsy.com/
UK Council for Child Internet Safety – Education for a Connected World

Appendix 1: Common Online Safety Issues

Online 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 online 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 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. Schools must have anti-bullying policies which articulate that participating in such activity will not be tolerated, and 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 online 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, and 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 online bullying, bystanders can easily become perpetrators – by passing on or showing to others images designed to humiliate, for example, or 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 online 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 contact the Director of Education who will assist you in contacting the Internet Service Provider to remove the content.

Involve the wider community. Schools are advised to provide parents and carers with information about online 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 13-20-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 your monitoring software flags up a term relating to self-harm, this must be responded to 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 Guernsey? 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 Guernsey 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 (if reported as a complaint to the police) 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 officer 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. Specific guidance and reporting procedures are detailed in Appendix 2

Appendix 2: Guidance 'Sexting' in Schools: Managing and reporting youth produced sexual imagery

Contents

1.0 Introduction

There are a number of definitions of sexting (or youth produced sexual imagery) but, for the purposes of this advice, it is simply defined as: 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. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

Creating and sharing sexual photos and videos of under-18s is illegal and therefore causes the greatest complexity for schools and other agencies when responding. It also presents a range of risks which need careful management. This advice will use the phrase 'youth produced sexual imagery' and uses this instead of 'sexting.' This is to ensure clarity about the issues this advice addresses. 'Youth produced sexual imagery' best describes the practice because:

'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.

'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.

'Imagery' covers both still photos and moving videos (and this is what is meant by reference to imagery throughout the document).

2.0 Handling Incidents

Disclosures in schools should follow the normal safeguarding practices and protocols. A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event.

When an incident involving youth produced sexual imagery comes to a school or college's attention:

- The incident should be referred to the Child Protection Officer, at the school / college, immediately
- Adults (apart from the designated Child Protection Officer) should not view youth produced sexual imagery unless there is good and justifiable reason to do so Wherever possible, the decision by staff to refer the matter to the Child Protection Officer, should be based on what they have been told about the content of the imagery
- The Child Protection Officer should hold an initial meeting with the young person involved to establish the facts
- 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. Parents / carers and students need to be told that the incident will be referred to the MASH

All incidents involving youth produced sexual imagery in schools / colleges must be reported to MASH. A MASH referral form must be completed (see Appendix A for guidance on the type of information to be included on the MASH form).

3.0 Securing Devices

Any devices involved need to be turned off and secured somewhere safe until the outcome of the MASH referral is known. If no further action is to be taken by MASH, the device should be returned to the student at the earliest opportunity and the images deleted (see 'No further Action from Mash' below– 1.) If the MASH and / or the Police take further action, the device will be detained by them until the incident has been fully investigated and an outcome reached.

Initial Review Meeting.
The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
- If a referral should be made to the police or the emergency duty team
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police or the emergency duty team should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13 You have reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

4.0 MASH

On receiving a referral from a school, the MASH will assess the risk to the child/ren and assess whether there any wider safeguarding concerns and decide on a course of action. If the incident has involved peer to peer sharing of a sexual image, the MASH is likely to take no further action and refer the case back to the school for them to deal with. If the incident is assessed as being more serious, and the child involved is at risk, the Police may become involved, the case may be referred to the convenor, Youth Justice or the locality teams for an assessment by a social worker. The school will be informed of the outcome of the MASH referral.

4.1 No further action from MASH

If, after reviewing the incident, MASH decide to take no further action and refer the case back to the school for them to deal with, the school must take the following action:

1. The student, involved in the MASH referral, and their parents/carers need to be informed of the outcome. The student must be directed to delete the image/s from their device/s and cloud storage (in the presence of the Child Protection Officer)
2. At the school's discretion, repeat offenders can be instructed not to bring their own devices into school
3. In an assembly, students must be told that an illegal image has been circulated at the school and, if they have the image/s on their devices, they must delete them
4. A letter must be sent home to parents /carers explaining that an illegal image has been circulated to students at the school and requesting them to talk to their children about it and ensure that all images are deleted
5. If appropriate, a restorative justice approach should be taken to resolve the matter with the students involved in sending / receiving the image/s

Further information and advice from the UK Council for Child Internet Safety (UKCCIS) can be found here

Appendix A: Information required for MASH referral form

Information required for MASH referral form:

1. Name and DOB of student and parents/carers
2. Is the student disclosing about themselves receiving an image, sending an image or sharing an image?
3. What sort of image is it? Is it of a severe or extreme nature?
4. How widely has the image been shared and is the device in their possession?
5. Is it a school device or a personal device?
6. Is there a significant age difference between the sender/receiver?
7. Has there been any external coercion involved?
8. Does the student need immediate support and or protection/ is the child more vulnerable / at risk than usual?
9. Are there other students and or young people involved, if so include details?
10. Do they know where the image has ended up?

Appendix B – Responding to Incidents of Youth Produced Sexual Imagery