Pan-Dorset

Online Safety Guidance

Contents:

1. Introduction

This procedure details what practitioners should do in the event of an online safety incident. It also covers what needs to be done if digital equipment is to be allocated to a young person. Staff and volunteers must follow the Safer Working Practice 2015 guidance and also the **Electronic Communication Procedure (Appendix A)** to minimise risk to young people and to themselves.

The variety of internet-connected devices is constantly changing but includes mobile phones, laptops, computers, tablets, smart TVs, webcams, cameras, games consoles and wearable technology, such as watches. Historically the websites, games and apps that could be accessed had specific and limited functionality. However, many now encompass social networking, messaging or other communication, uploading of images and videos, live web cam streaming within one app so the issues are consequently more complex.

It can be helpful to consider risks on the internet as falling into one or more of the following categories: exposure to inappropriate content, exposure to unknown or inappropriate contacts and conduct, either by young people or by their contacts that puts them at risk. In particular, young people may be unaware of the risks of sharing personal information, contacting strangers or the importance of privacy settings in protecting themselves.

2. General Management of Incidents Involving Digital Media

The following section gives general advice about managing an online safety incident. This general procedure also covers online safety incidents such as hacking or unauthorised access, which will be defined by the organisation's acceptable use policy hacking (and might constitute offences under the Computer Misuse Act 1990) where a young person is the instigator. For information regarding specific types of incident see the information in the sections below.

If the instigator is a member of staff or volunteer, then disciplinary, measures should be considered and where there has been harm to children, or the behaviour indicates the person may be unsuitable to work with children this should be managed using the **Allegations Against Staff and Volunteers Procedure**.

If the victim is a member of staff or volunteer then this incident should be managed using organisational support services.

The general procedure for managing incidents is as follows:

- Refer to online safety, safeguarding, acceptable use and any other relevant organisational procedure;
- Decide on appropriate action – deal with using local procedures, or refer to Local Authority Children's Services and/or Police and preserve evidence/hardware;
- Take action, record appropriately;
- On completion, review actions to see if any organisational procedures need to be changed.

See also: **Flowchart for Managing Incidents Using Digital Media** (Appendix B). The notes below accompany the Flowchart.

For the victim, consider the following issues:

- Is there further risk of harm?
- Have the parents/carer been informed?
- Should the victim be referred to Children's Services as a Child in Need?

- Should a CAF be done to provide support services to the child?
- What are the support needs / vulnerabilities of the child?

If the instigator is also a child:

- Do the Child Protection Procedures apply in respect of the instigator?
- Have the parent/carer be informed?
- Should there be a Risk Assessment of circumstances surrounding the child?
- Should the child be disciplined or provided with guidance/advice/support?
- Should the child's access to technology be monitored /curtailed in the future?

Serious online safety incidents (e.g. sexting, grooming, child sexual exploitation, serious threats made or significant risk harm to the victim, or where a person 18 or over is involved) must be referred to the police via the normal referrals procedure. Incidents that fall within the Dorset Police Youth Internet Safety Policy, i.e. only involve young people under 18 and are not serious may be referred directly from schools to the Safe Schools and Communities Team via the Dorset Police Triage Service.

3. Online Bullying

Definition

Bullying is behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally. Note that some organisations define bullying as including an imbalance of power. Schools and other agencies will have their own definitions of bullying, which must be communicated to young people, parents and professionals. However, some cases that are one-off incidents, for example friendship issues, may be perceived as bullying by the victim and may therefore need to be dealt with.

Online bullying, sometimes referred to as cyberbullying, is bullying that occurs via digital technology, whether that be messenger apps, social media such as Facebook or Instagram or even gaming platforms such as Xbox or PlayStation. It includes but is not limited to:

- Sending threatening or abusive messages;
- Creating and sharing embarrassing images or videos;
- 'Trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games, whether this is from a known or unknown person;
- Excluding someone from online games, activities or friendship groups;
- Setting up hate sites or groups about a particular person;
- Encouraging young people to self-harm;
- Voting for or against someone in an abusive poll;
- Creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

Online bullying has additional issues from offline bullying in that it can happen at all times of the day, there can be a huge audience witnessing the bullying and that it can escalate quickly at the click of a button. Furthermore the content of the bullying can be more unpleasant as perpetrators hide behind the anonymity of the internet. Some online bullying includes prejudice against particular groups, for example

on grounds of race, religion, gender, sexual orientation, disability, or because a child is looked after, adopted or has caring responsibilities. Still other online bullying may include threats to harm or kill.

Risks

There are impacts for both victims of bullying and those children and young people who bully. According to Kidscape, children who are bullied are more likely to:

- Have low self-esteem;
- Develop depression or anxiety;
- Become socially withdrawn, isolated and lonely;
- Have lower academic achievements due to avoiding or becoming disengaged with school;
- Be unable to form trusting, healthy relationships with friends or partners in the future.

Children who frequently bully others are more likely to:

- Drop out of, or be expelled from school;
- Engage in criminal behaviour;
- Develop depression or anxiety;
- Be abusive towards their sexual partners, spouses or children as adults.

Bystanders who experience others being bullied may also have feelings of guilt and powerlessness.

Indicators

Young people may report to an adult that they are being bullied online although research suggests that the majority of online bullying is not reported by young people. Online bullying may be reported by a young person's friend or their parents/carers seeing the bullying occurring online. It is not always easy to spot signs of online bullying. However parents/carers and professionals should be alert to changes in behaviour. The following may also be signs of online bullying:

- Being upset after using the internet or their mobile phone;
- Unwilling to talk or secretive about their online activities and mobile phone use;
- Spending much more or much less time texting, gaming or using social media;
- Many new phone numbers, texts or e-mail addresses show up on their mobile phone, laptop or tablet;
- After texting or being online they may seem withdrawn, upset or outraged;
- Not wanting to go to school and/or avoiding meeting friends and school mates;
- Avoiding formerly enjoyable social situations;
- Difficulty sleeping;
- Low self-esteem.

These indicators may also apply to on-line grooming, so practitioners need to vigilant about the range of implications.

Protection and Action to be Taken

Very little online bullying is a police matter. Organisational responses to online bullying should be covered in the relevant organisational policies, for example acceptable use, behaviour, child protection, safeguarding, and anti-bullying policies. This must include recording procedures, including additional procedures required when dealing with incidents involving prejudice against a particular group.

State schools have a statutory responsibility to deal with bullying incidents, including online bullying even where it has happened away from school (Section 89 of the Education and Inspections Act 2006). Where a young person or parent/carer reports to the school that they are being bullied, the schools anti-bullying policy should be used to resolve the situation wherever possible. Where the other parties are within the school, this should be relatively straight-forward to deal with. If the perpetrators of the bullying attend another school and their names and school are known, this information should be passed to the other school to deal with. If the young person is being bullied by an unknown person and this has happened over a period of time, the school should report this to the police. The school will still need to support the victim.

Not all online bullying incidents must be reported to Children's Services or police: while following the relevant procedures, the agency dealing with the incident must carry out a risk assessment to determine if the incident needs referring to Children's Services and/or the police. Under the Children Act 1989 a bullying incident should be addressed as a safeguarding concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm'.

The agency dealing with the incident should provide appropriate advice to the young person and parents/carers including, but not limited to, blocking and deleting people from their contacts list and how to get the content removed from websites using the reporting functions available. Consideration must be given to safeguarding the young person taking into account parents' concerns about use of the device and internet access.

If the material has been reported to the website, game or app via their reporting tools and the material has not been removed, then the agency should consider contacting the **Professionals Online Safety Helpline** who may be able to assist. The agency should also provide advice to both victims and perpetrators about how to prevent online bullying in future. Practitioners will need to deal with victims, perpetrators and bystanders of this behaviour.

Child protection concerns must be referred to Children's Services in line with the Referrals Procedure.

Where appropriate the incident must be referred to the Police in line with the Referrals Procedure: it is generally proportionate to refer any online bullying incidents to the police where the incident could potentially lead to a criminal investigation, for example incidents where threats are made to the victim, incidents involving harassment over a period of time or anything involving hate crimes.

Police Action

There is no specific offence of online bullying. However there a number of existing laws that can be used to prosecute cases of online bullying and harassment, for example Protection from Harassment Act 1997, Criminal Justice and Public Order Act 1994 or Malicious Communications Act 1988 (see Legal Information). It is unlikely that a young person will be prosecuted in relation to online bullying. The current CPS Guidelines on prosecuting cases involving communications sent via social media issued 20 June 2013 state that 'The age and maturity of suspects should be given significant weight [in deciding whether to prosecute], particularly if they are under the age of 18. Children may not appreciate the potential harm and seriousness of their communications and a prosecution is rarely likely to be in the public interest.'

Therefore, not all cases of online bullying involving young people will be investigated. A significant number will be passed to the Safer Schools and Communities Team to liaise with parents/carers and schools to respond under their anti-bullying and behaviour policies.

Online bullying Incidents Where the Victim is an Adult (Member of Staff/Volunteer)

Where the victim of online bullying is a member of staff, it is essential that the member of staff follow the appropriate procedures within the agency. If the agency refers to the police, this may be dealt with as a Schools Incident or as a general online safety incident. Again, the **Professionals Online Safety Helpline** may be able to assist with removal of material from websites.

4. Sexting or Youth produced sexual imagery

Definition

There is no agreed definition of 'sexting' and the fact that creating and sharing sexual photos and videos of under-18s is illegal (see 9. **Legal Information** below) causes complexities for schools and other agencies when responding. New non-statutory guidance produced by the UK Council for Child Internet Safety *Sexting in schools and colleges: Responding to incidents and safeguarding young people has now replaced the previous guidelines Sexting in schools: advice and support around self-generated images*. The new guidance introduces the phrase 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).

It covers:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18;
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult;
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

Sharing of this type of imagery by and between young people often occur when a young person has taken an image or video of themselves and sent it to their boyfriend or girlfriend via their mobile phone. Alternatively, young people may create and distribute images as a way of seeking sexual attention; this is often referred to as 'experimental'.

More seriously, where an adult is involved or where there is only youth involvement but that there is some intent to harm or where the images are taken without consent, 'reckless misuse', this is described as 'aggravated'.

Risks

There are many reasons why a young person might get involved in sexting. Exploring sex and relationships is a natural part of adolescence. However, sometimes they might be put under pressure to either take pictures of themselves or pass on those taken by others: many young people now accept this behaviour as normal.

Young people may also be coerced into taking and sending images by an adult or someone they've met online.

As the young people have no control over how and where images and messages might be shared online by other people, sexting can leave them vulnerable to bullying, humiliation and embarrassment, blackmail for further images, and even to self-harm and suicide. It should be noted that these types of self-generated images are more commonly being found in collections of images stored by child sex offenders.

Indicators

It is likely that one or other of the parties involved, or possibly a third party who has seen or is aware of the image, will disclose the existence of the image to an adult.

Enquiries into any incident of this nature must be carried out according to the relevant organisational policies and procedures (for example, internet safety, acceptable use, behaviour, child protection and safeguarding, anti-bullying) and should always be recorded by the child protection officer/safeguarding lead.

There should be clear sanctions where the policies are breached.

Searching a Device, Viewing and Deleting Imagery

An image may have been potentially shared via multiple devices and websites. It is important to establish the location of the image, but be aware that this may be distressing for the young person involved.

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 kept securely until the police are able to come and retrieve it.

An image may have been potentially shared via multiple devices and websites. It is important to establish the location of the image, but be aware that this may be distressing for the young person involved.

Teachers and schools have powers to examine, confiscate and store a device if it is believed to contain indecent images/imagery of this nature. However no material may be printed from the device or shared with another device. The image should not be viewed unless there is a clear reason to do so and the device should be stored securely. Devices should not be searched until relevant colleagues and senior management team/Headteacher have been informed. The Designated Safeguarding Lead should view the imagery with the presence of another member of staff in the room, ideally the Headteacher or member of the senior leadership team. Ideally the member of staff viewing the images should be the same sex as the person in the imagery. Record the viewing of the imagery including justification for why the image needed to be viewed. However no material may be copied, printed or shared. printed from the device or shared with another device.

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. However, just as in most circumstances it is not recommended that school staff view imagery, it is recommended that schools should not search through devices and delete imagery unless there is good and clear reason to do so.

It is recommended that in most cases young people are asked to delete imagery and to confirm that they have deleted the imagery. Young people should be given a deadline for deletion across all devices, online storage or social media sites. Young people should be reminded that possession of youth produced sexual imagery is illegal. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the young person.

For further information see Searching, Screening and Confiscation advice.

Protection and Action to be Taken

- Ensure the incident is recorded;
- Carry out a risk assessment in relation to the young people involved;
    - Do you have any concerns about the young person's vulnerability?
    - Why was the imagery shared? Was it consensual or was the young person put under pressure or coerced?
    - Has the imagery been shared beyond its intended recipient? Was it shared without the consent of the young person who produced the imagery?
    - Has the imagery been shared on social media or anywhere else online? If so, what steps have been taken to contain the spread of the imagery?
    - How old is the young person or young people involved?
    - Did the young person send the image to more than one person?
- If this is an incident where there has been significant harm then it must be referred to Children's Services in line with the Referrals Procedure; also if you are aware that the young person is involved Children's Services with or have been in the past then contact them;
- Where appropriate the incident must be referred to the Police in line with the Referrals Procedure: it is generally proportionate to refer any incidents to the police which involve one or more of the following: adults involvement; coercion or blackmail; extreme or violent; under 13 or at immediate risk of harm;
- Where the incident will be managed within the school, the Designated Safeguarding Lead will likely need to speak to the young person or people involved and discuss any relevant issues. Parents/carers should usually be informed at the earliest possible stage unless this will put the young person at risk. Note that some parents/carers will require support to ensure they deal with this issue appropriately. Put the necessary safeguards in place for all the young people involved, e.g. appropriate education, counselling or parents being informed;
- Where relevant, assist a young person to report imagery that has been posted online. Most online service providers now provide tools for this. If the site provides no tool, you should report it to the **Internet Watch Foundation (IWF)**. Young people can report to Childline, who will work with the IWF to support the young person;
- If there are inappropriate images of a child on a website or social networking site, contact the **Professionals Online Safety Helpline** run by the UK Safer Internet Centre for assistance in getting these removed;
- Ensure the incident is recorded appropriately. If it has been managed within the school ensure all the reasons for this are documented.

Police Action

The National Police Chief's Council has made clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues.

Where there is any suggestion of coercion or adult involvement then the incident will be routed to the Safeguarding Referral Unit to investigate to see if a criminal justice response is required. Following the investigation, an educational response may be provided. Many reports to Dorset Police will usually be routed to the Safe Schools and Communities Team who will provide the education on a 1-to-1, small group or larger group basis without the need for a criminal investigation.

However, it is important to note that some reports to the police will be entered onto the crime system with the young people involved being named. This is not the same as a criminal record and most are finalised with a decision not to take any formal action due to it not being in the public interest. It is very unlikely that these cases of youth produced sexual imagery would ever be disclosed on a Disclosure and Barring Service Certificate; however it isn't possible to say categorically that this information would never be disclosed on an Enhanced Criminal Records check.

Issues

Although many online safety campaigns are aimed at reducing the danger to young people from strangers, youth produced sexual imagery is predominantly an issue relating to pressure from a young person's peers and friends so different approaches may be required to support young people facing these issues. In addition, elements of online bullying and coercion may be present and young people may face isolation or bullying if they try to resist taking part.

While this behaviour is often regarded by young people as the norm and nothing to worry about, the consequences can be devastating for young people. Technological advances mean that once an image has been shared on the internet it may be viewed and shared by others outside the original peer group. Of particular concern is the increase in the number of self-generated images now being identified by law enforcement when searching devices belonging to online sex offenders.

5. Viewing or Uploading Inappropriate Material

Definition

Incidents involving the viewing or uploading of inappropriate material may happen accidental or deliberate. The types of material that are considered inappropriate include but are not limited to images of a sexualised nature featuring adults, material relating to eating disorders or self-harming/suicide, sites encouraging violence and hate, or material that might be capable of radicalising a young person.

Where a person is viewing indecent images of young people under 18 years old or child sexual abuse images these are illegal and will be subject to a criminal investigation.

Where a person is uploading material, it may be that the material may not be illegal or put them at a high risk of abuse, but it may increase their vulnerability to being targeted: for example, uploading a video of themselves to YouTube where they are wearing their school uniform or taking part in discussions on an inappropriate website.

All regulated online pornography websites try to prevent under 18s from accessing them. The government has recently clarified existing obscenity laws to ensure that materials rated only suitable for 18 year olds (and above) have controls in place to stop children under 18 from accessing them. There are certain types of pornography that are illegal – even for an adult to be in possession of. These are called "extreme pornographic images", and include acts that threaten a person's life, acts which are likely to, or, result in serious injury, degrading pornography, violent pornography (which includes rape and abuse) or anything involving those under the age of 18. Any images of child abuse are illegal and these should be reported immediately to the **Internet Watch Foundation**, which has responsibility for removing them.

The Pan European Games Information rating system provides guidance as to whether a video game is appropriate or not. The possible age ratings are 3, 7, 12, 16 and 18 and there are further ratings indicating whether the game contains violence, fear, drugs, bad language, sex, discrimination, gambling, and online gaming. These symbols can be found on all games sold in packaging and is now also found on downloadable games from the Google PlayStore, Apple Store etc. In addition, other apps can have ratings defined by the British Board of Film Classification (BBFC).

Risks

There are a number of reasons why young people will access online pornography, including: wishing to learn about sex and sexual identities, curiosity, a want to be sexually aroused, for "a laugh", to break the rules, to be disgusted or to "freak out" their friends (NSPCC).

Research shows that exposure to pornographic content can have significant negative effects on young people including:

- Unrealistic attitudes about sex and consent;
- More negative attitudes towards roles and identities in relationships;
- More casual attitudes towards sex and sexual relationships and increase in 'risky' sexual behaviour;
- Unrealistic expectations of body image and performance.

In relation to inappropriate material that is not related to sexual content, there are still risks associated with viewing and uploading material to these types of sites. There are some sites and online communities where people with anorexia or other eating disorders go to post pictures of themselves and share tips on losing weight. So-called ‘Pro-ana’ websites or 'thinspiration' blogs can be really harmful and negative places as they can encourage people to get dangerously underweight. A young person might believe that these websites are a good way to talk to people who know what they’re going through; however, these sites often make eating problems worse. These sites may also present anorexia or bulimia as a choice rather than a mental illness that can be recovered from. In addition, someone deciding to leave such a site may feel guilty that they are failing to support someone else at risk (Childline). Similar concerns exist in relation to self-harm/injury sites.

Radical and extremist groups may use social networking to attract children and young people into rigid and narrow ideologies that are intolerant of diversity: this is similar to the grooming process and exploits the same vulnerabilities. The groups concerned include those linked to extreme Islamist, or Far Right/Neo Nazi ideologies, Irish Republican and Loyalist paramilitary groups, extremist Animal Rights groups and others who justify political, religious, sexist or racist violence. Children may be drawn to adopt a radical ideology through a failure to appreciate the bias in extremist material; in addition by repeated viewing of extreme content they may come to view it as normal. Young people may self-radicalise by seeking out material themselves or may be groomed in a process similar to that involved in child sexual exploitation.

The risks of online gaming are less clear. Children who play games with PEGI ratings older than their age group may find content that is potentially upsetting. For example, violent or sexualised content or bad language that may be OK for an adult is more likely to upset a young child. Sometimes the viewpoints or behaviour experienced in the games may be copied by children and taken into another environment which can cause risks for other children. Games that can be played over the internet carry the same risks in relation to contacting strangers and conduct risks of bullying or people trying to engage a young person in inappropriate behaviour.

Indicators

A young person or their friends may disclosure the content that they have been viewing or uploading or it may be discovered by family, friends or professionals working with the young person or potentially by one of the monitoring strategies a parent/carer may have put in place.

A young person involved with an online community may withdraw from off line communities or family and be focussed heavily on the online community, or they may repeat the views of the online community.

Protection and Action to be Taken

Incidents falling under this category vary greatly in their seriousness and the likely harm to a young person. Practitioners must follow safeguarding procedures in conjunction with these procedures to decide on the most appropriate course of action. Incidents that fall within the Dorset Police Youth Internet Safety Policy, i.e. only involve young people under 18 and are not serious may be referred directly to the Safe Schools and Communities Team: other online safety incidents should be referred to the police via the normal Referrals Procedure.

Where there are concerns in relation to a child's exposure to extremist materials, procedures around Prevent will be followed (see Pan-Dorset Multi Agency Safeguarding Procedures -**Prevent: Safeguarding Children and Young people against Radicalisation and Violent Extremism**). Content of concern can also be reported directly to social media platforms – see **www.saferinternet.org.uk**.

6. Grooming and Sexual Abuse Using Digital Media

Definition

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. Children and young people can be groomed online or in the real world, by a stranger or by someone they know - for example a family member, friend or professional. Groomers may be male or female. They could be any age. Many children and young people don't understand that they have been groomed, or that what has happened is abuse (NSPCC).

When sexual exploitation happens online, young people may be persuaded, or forced, to send or post sexually explicit images of themselves; take part in sexual activities via a webcam or smartphone; or to have sexual conversations by text or online.

Social networking sites or other communications apps are often used by perpetrators as an easy way to access children and young people for sexual abuse. However any website, game or app that allows communication can be used to groom or abuse a young person.

Some perpetrators will use the internet to groom one or more young people but their aim is to meet the young person offline for abuse.

For more information see chapter: **Child Sexual Exploitation – Pan-Dorset Multi Agency Safeguarding Procedures**

The procedures relating to **Organised and Complex Abuse** and **Allegations Against Staff and Volunteers** should be borne in mind depending on the circumstances of the concerns.

See also **Appendix C - Youth-Produced Sexualised Image (Sexting) Guidance Flowchart for Action Outcomes**.

Risks

There is some evidence that people found in possession of indecent photographs/pseudo photographs or films/videos of children may now or in the future be involved directly in child abuse themselves. In particular, the individual's access to children should be established to consider the possibility that they are actively involved in the abuse of children including those within the family, within employment contexts or in other settings such as voluntary work with children or other positions of trust. Any indecent, obscene image involving a child has, by its very nature, involved a person, who in creating that image has been party to abusing that child.

Children may be groomed for sexual exploitation on-line.

Indicators

Often these issues come to light through accidental discovery of images on a computer or other device. The initial indicators of abuse are likely to be changes in behaviour and mood of the victim. Clearly such changes can also be attributed to many innocent events in a child's life and cannot be regarded as diagnostic. However, changes to a child's circle of friends or a noticeable change in attitude towards the use of computer or phone could have their origin in abusive behaviour. Similarly, a change in their friends or not wanting to be alone with a particular person may be a sign that something is upsetting them.

Children often show us rather than tell us that something is upsetting them. There may be many reasons for changes in their behaviour, but if we notice a combination of worrying signs it may be time to call for help or advice.

Protection and Action to be Taken

Where there is suspected or actual evidence of anyone accessing or creating indecent images of children this must be referred to the Police in line with the Referrals Procedure.

Where there are concerns about a child being groomed, exposed to pornographic material or contacted by someone inappropriately, via the Internet or other ICT tools like a mobile phone, referrals should be made to the Police and to Children's Services in line with the Referrals Procedure.

The Serious Crime Act (2015) has introduced an offence of sexual communication with a child. This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years of age. The Act also amended the Sex Offences Act 2003 so it is now an offence for an adult to arrange to meet with someone under 16 having communicated with them.

Due to the nature of this type of abuse and the possibility of the destruction of evidence, the referrer should first discuss their concerns with the Police and Children's Services before raising the matter with the family. This will enable a joint decision to be made about informing the family and ensuring that the child's welfare is safeguarded.

All such reports should be taken seriously. Most referrals will warrant a Strategy Discussion to determine the course of further investigation or enquiry. Intervention should be continually under review if further evidence comes to light.

Issues

When communicating via the internet, young people tend to become less wary and talk about things far more openly than they might when communicating face to face. Both male and female adults and some young people may use the internet to harm children. Some do this by looking at, taking and/or distributing photographs and video images on the internet of children naked, in sexual poses and/or being sexually abused.

Children and young people should be supported to understand that when they use digital technology they should not give out personal information, particularly their name, address or school, mobile phone numbers to anyone they do not know or trust; this particularly includes social networking and online gaming sites. If they have been asked for such information, they should always check with their parent or other trusted adult before providing such details. It is also important that they understand why they must take a parent or trusted adult with them if they meet someone face to face whom they have only previously met on-line.

Children also need to be made aware of the risks involved in sending naked images of themselves to others – sexting.

7. Allocation of Digital Equipment to a Young Person

Advances in internet technology and connectivity have created significant opportunities for children and young people such as access to on-line materials, virtual learning platforms and greater opportunities to communicate and socialise in the virtual world. However, we know there are risks and dangers associated with this as described above.

There will be occasions where computers or other digital devices will be issued to children and young people. This protocol has been developed to assist professionals to minimise the risks to the young people, particularly where they will have unsupervised access to the computers (e.g. laptops that they use outside of the organisation).

It is the responsibility of organisations working with children and young people to have their own safeguarding policy and online safety policies that cover how professionals are expected to work in order to protect young people and themselves where digital technology is used. These should be consistent with this Pan-Dorset online safety policy.

At **Appendix D** there is a template letter that can be used where digital equipment is to be allocated to a young person.

Prior to issuing digital equipment

- Ensure the hardware has been cleaned and nothing remains on the equipment from the previous user;
- Ensure approved filtering software is installed;
- Inform the Safe Schools and Communities Team (SSCT) who can visit to offer advice and support on online safety. This includes, if necessary, visiting the young person's home. Tel: 01202 222844 or E-mail: **ssct@dorset.pnn.police.uk**.

On issuing the digital equipment

- Provide up-to-date and age appropriate information to the young person regarding the potential dangers associated with internet use. Useful websites to assist with online safety are given in the Further information section;
- Provide parent/carers, schools and other organisations with details on how to obtain free software giving guidance on parental monitoring. This can be found via the internet provider;
- Make it clear whether the equipment now permanently belongs to the young person or whether it is on loan and remains the property of your organisation;
- If the equipment remains the property of your organisation, it would be good practice for an annual check to be carried out regarding how it has been used. If any concerns are raised, advice can be sought from the Safe Schools and Communities Team;
- Anti-malware software will only protect the system if it is up-to-date. Digital equipment therefore needs to be connected to the internet on a weekly basis in order to automatically up-date;
- Encrypted memory sticks containing sensitive information should be stored in a secure manner and never left in the equipment.

8. Further Information

- **UK Safer Internet website**
- **CEOP website**
- **ThinkUknow website**

- **Child Safety Online: A practical guide for parents and carers whose children are using social media**

Online bullying

Organisations who work in the general field of bullying are listed on the Bullying protocol.

Specialist online bullying organisations include:

- **Cybersmile Foundation**: Founded in 2010, by the parents of children directly affected by online bullying, the non-profit organisation is committed to tackling all forms of digital abuse and bullying online, by working to promote diversity and inclusion by building a safer, more positive digital community. It also runs 'Stop Cyberbullying Day' each year in June.
- **ChildNet International**: Specialist resources for young people to raise awareness of online safety and how to protect themselves.
- The government has produced a number of guidance documents for schools on **Preventing Bullying** and Bullying at School.

Sexting

- **Searching, screening and confiscation: Advice for head teachers, school staff and governing bodies (January 2018)**.
- UKCCIS (2016) 'Sexting' in schools: advice and support around self-generated images: What to do and how to handle it (March 2013) available from the CEOP website. **Responding to sexting in schools and colleges – UKCCIS Guidance**.
- **NSPCC (2012) A qualitative study of children, young people and 'sexting'**.
- Educational material can be found at **www.thinkuknow.co.uk**.

Viewing and uploading inappropriate material

- **BBFC regulation of mobile content**
- **BBFC digital age ratings**
- **NSPCC information about viewing online pornography**
- **Grooming and sexual abuse using digital media**
- **Child Exploitation and Online Protection Agency**

9. Legal Information

Behaviour that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation. The following legislation may apply:

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;

- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;

- Ensure the effective operation of the system;
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal;
    - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 on one occasion (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with

any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health practitioners, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

The Education and Inspections Act 2006

Empowers school Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Serious Crime Act 2015

The Act introduces a new offence of sexual communication with a child. This would criminalise an adult who communicates with a child for the purpose of obtaining sexual gratification, where the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16.

Appendix A

Pan-Dorset Guidelines for communicating with children and young people

These Guidelines for Text Messaging, e mailing and e safety are produced to complement the Keeping Children Safe in Education 2016. The guidance document was commissioned by the Department for Education (DfE). It does not replace or take priority over advice or codes of conduct produced by employers or national bodies. It is a generic document that should complement existing professional procedures, protocols and guidance which relate to specific roles, responsibilities or professional practices.

The section that applies to technology is page 17 of Keeping Children Safe in Education 2016.

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. This means that the organisation should have a communication policy which specifies acceptable and permissible modes of communication.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. Email or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This means that adults should:

- *not give their personal contact details to children or young people, including their mobile telephone number (unless agreed as part of your organizations policy*
- *only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used*
- *only make contact with children for professional reasons and in accordance with any organisation policy*
- *recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible*
- *not use internet or web-based communication channels to send personal messages to a child/young person*

GUIDELINES FOR TEXT MESSAGING AND E MAILING

Whilst these guidelines refer specifically to text/email communication, all staff should be aware of the need for appropriate professional recording and boundaries in ALL communication with children and young people, whether written or oral.

1. TEXT MESSAGING

1.1 A written record should be made of all calls from/to a mobile phone in the same way as calls from a landline, according to agency/service procedure.

1.2 It is good practice to make a specific note of any mobile phone contact outside of normal working hours.

1.3 Work mobile numbers should only be given out to children/young people in accordance with agency/service protocols and policies. Line managers should be informed of all occasions when a number is given.

1.4 The use of texting is accepted as an essential tool of social contact for young people. Adult users must be aware of this. It is recognised that texting is increasingly becoming a 'normal' professional tool of communication between adults and young people alongside meetings, telephone calls and letters.

1.5 Texting should only contain information of a professional nature and written plain, unambiguous language, reflecting dialogue that would occur face to face. The language used should be professional and appropriate to the service/agency. It would not be appropriate to use 'text language' in a professional communication.

1.6 Texting should only be used if previously agreed by the child/young person e.g. for a specific agreed reason or purpose. The reason should be noted in the case record.

1.7 Texting should not normally be used as third party communication i.e. to ask one service user to pass on a message to another service user.

1.8 All texts sent/received must recorded by being transcribed and put in the case file, timed and dated when recorded.

1.9 It is not recommended that personal home or mobile numbers are given to children or young people (or any service user). This should only happen where a service/agency policy specifically allows it and should be agreed with the line manager.

1.10 Any texts/calls of an abusive, threatening or nuisance calls should be recorded and reported to line manager.

1.11 Agencies/services should be clear about when a work mobile should be switched on or off. A nuisance call received out of work hours can be very distressing. If the phone is off no nuisance call can be received.

1.12 The law is very clear about the use of mobile phones when driving, all users have a responsibility to comply with the law. Some agencies/authorities instruct that all mobiles are switched off when driving.

1.13 It is possible for mobile phones with Bluetooth capability to receive unsolicited material, including images. Any such images received should be reported to line manager and then deleted. Please be aware that the Bluetooth issue is a complex one, all phones differ. Mobile phones can be configured to prevent unsolicited material. Please contact your provider to clarify this.

2. POLICE ADVICE REGARDING INDECENT VIDEO, FILM OR STILL IMAGES TRANSMITTED BY MOBILE PHONE

2.1 No young person should be asked to forward any material by staff as this is inadvertently asking the young person to commit an offence of distributing indecent images.

2.2 If a young person is volunteering the images for a member of staff to view the staff member should get the young person's permission to hold on to the phone and contact the police to see if they want to view the images.

2.3 If a staff member has an image received on their phone they should contact their Headteacher/Line Manger/Head of Service immediately so that a manager is aware that the image has been received. The police can then be contacted and the image viewed by them if necessary and then deleted

2.4 If a young person refuses to give their phone to a member of staff the young person should be advised to delete the material and a record of such kept on the agency file. The same advice should be given to staff.

2.5 SCHOOL STAFF SHOULD NEVER DOWNLOAD ANY INDECENT MAGES BUT IF IN DOUBT OF THE CONTENT, CONTACT THE POLICE Multi Agency Safeguarding Hub (MASH) SRU (Safeguarding Referral unit), OR DESIGNATED MEMBER OF STAFF FOR SAFEGUARDING WITHIN THE LOCAL AUTHORITY.

3. EMAIL COMMUNICATION

3.1 Many young people and children have a personal e mail address.

3.2 Any adult working with children or young people should only use a work email address, as defined by service or agency.

3.3 Any communication by e mail must be compliant with any individual service/agency protocol and guidance.

3.4 All communication should be for clear professional reasons and the content must reflect this.

3.5 E mail communication should only be used as part of an agreed strategy or plan with the child/young person and parent/carer should be aware of this, according to age of young person and agency/service protocol and guidance. Any e mail communication without parent/carer knowledge should only happen with the agreement of a line manager and the decision recorded

3.6 A record of all e mails sent/received should be kept as part of the agency add ‘or service’ record, printed off or copied into a computer system.

4. SOCIAL NETWORKING SITES

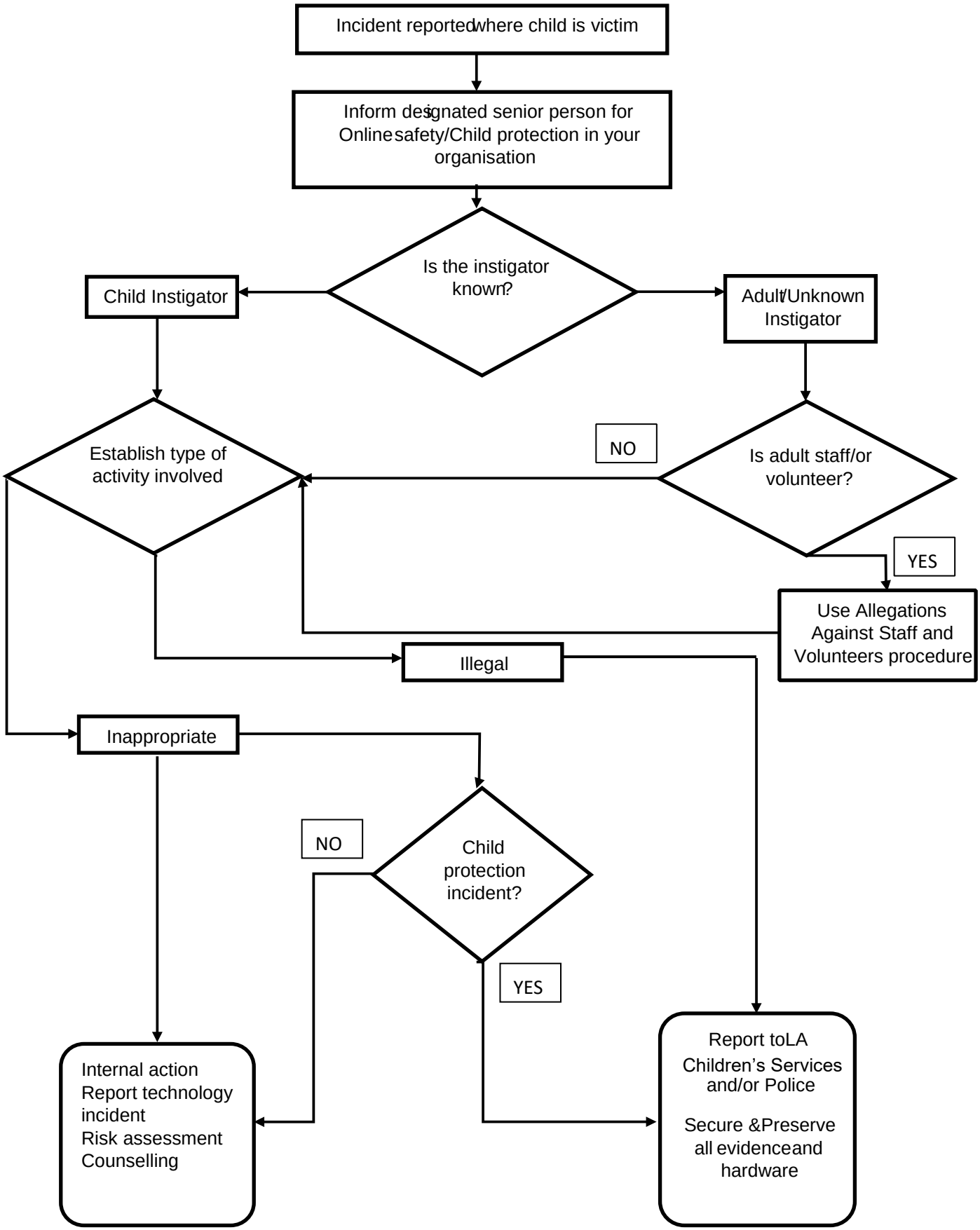
4.1 It is not recommended that adults working with children/young people correspond through social networking sites.

4.2 If you become aware of a social networking site which contains any personal information about activities of concern about a young person known to you, this should be recorded and the line manager should be informed.

4.3 Staff should be aware of possible implications when entering any personal details on any gaming or social networking site e.g. you tube, my space, facebook etc.

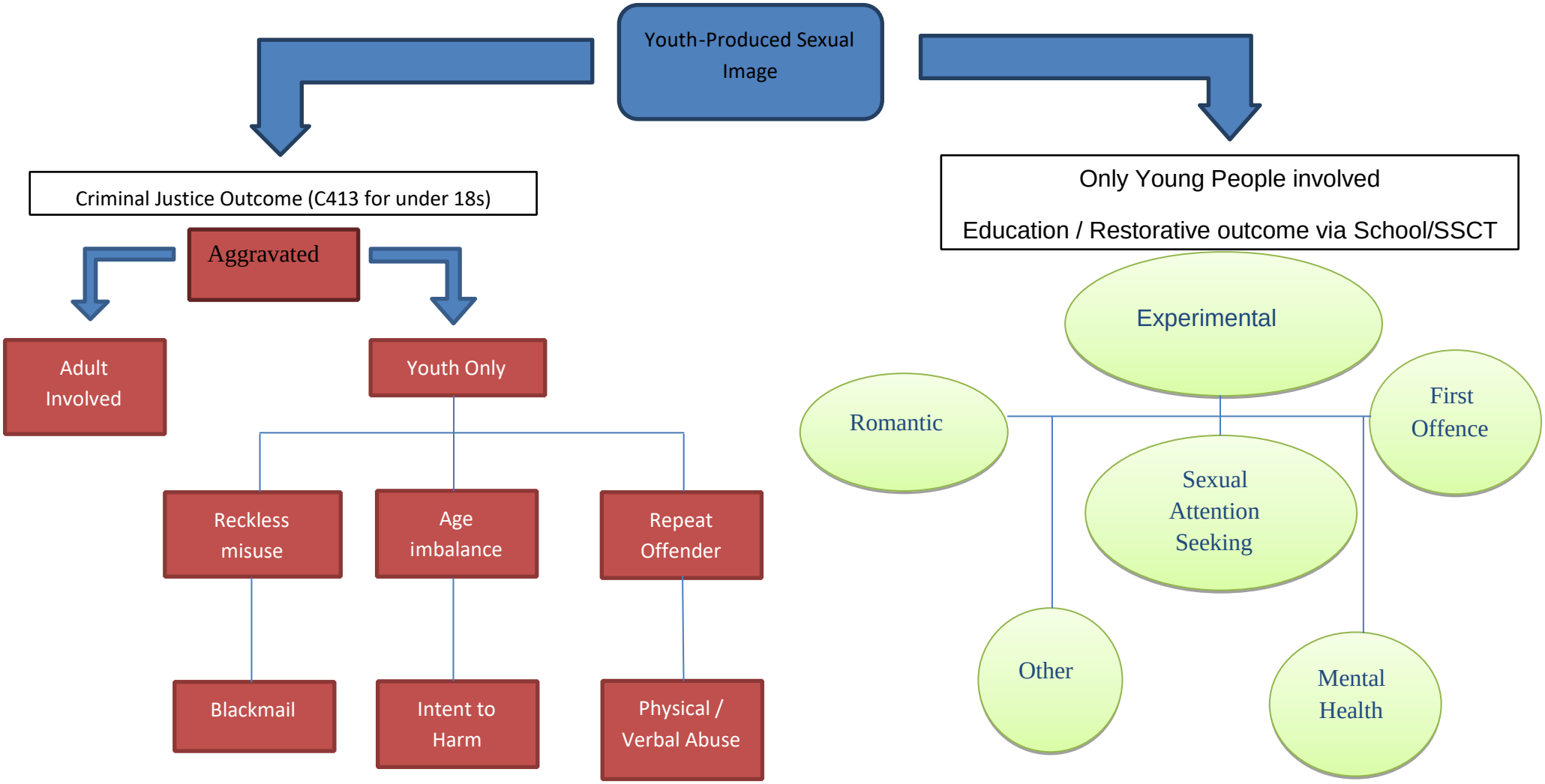
Appendix B

Managing incidents using digital media



Appendix C

Youth-Produced Sexualised Image (Sexting) Guidance Flowchart for Action Outcomes



Appendix D

[DATE]

Dear

Re: ***[name & d.o.b. of child]***

Following discussion, it has been agreed to provide the following special equipment for the above child to use. The equipment will be supplied directly to *[name of organisation or venue].*

Please telephone me when the equipment has been delivered. If the equipment has not been received within 21 days of this letter please contact me.

This equipment is for specific use by the above named child whilst s/he attends your organisation and should be returned to you when the above child no longer attends your organisation or no longer has use for it.

The equipment remains the property of the *[name of organisation]* and all concerned are asked to make every effort to care for the equipment.

Please refer to the Pan Dorset Interagency E-safety procedures which gives advice on all details relating to the equipment and outlines the actions required to ensure the children and young people are kept safe on line.

Arrangements will be made to regularly review this allocation of equipment. Should you have any queries about the loan of this item please do not hesitate to contact me.

Yours sincerely

[Name of provider]