3Dimensions

Jun-18

Internet Access and Online Safety

INTERNET ACCESS, SOCIAL MEDIA AND ANTI-CYBERBULLYING FOR INDIVIDUALS IN OUR CARE

Document Classification
INTERNAL

3Dimensions

Policy version control sheet

Document status	Current
Policy Number	52
Version Number	V1.0
Date of Policy	10 June 2018
Next review date	May 2019
Name of originator	Shaun Davis
Approved by	Nita Ellul
Date of approval	11.06.2018
Target Audience	Staff Referring authorities Parents and carers Regulatory bodies Individuals in our care
Links to other policies	All other Data Protection and IT related Policies

Changes to previous version
This policy has been extensively updated and replaces Internet Access and Social Media for Young People and Vulnerable Adults, and Anti-Cyberbullying.

Distribution		
Intranet	Website	Email to managers
✓		
Unless this version has been taken directly from the 3 Dimensions website, there is no assurance that this is the correct version.		

Definitions

Term	Definition
Must	This term is used to state a Mandatory action
Should	This term is used to state a Recommended action
Individuals in our care	Any individual within our care includes all young people who reside within our house or attend our school and any housemates who reside in our adult care provision.
ICT facilities	All computers, laptops, tablets, smartphones, smart TVs, games consoles and other electronic devices which can access the internet, which 3 Dimensions own or manage

1 Policy Outline

1.1 Introduction

1.1.1 The use of computers, social media and the internet within the home and school supports learning, social development and brings opportunities to engage and communicate in new ways. However, it is also important to ensure within our care are safe whilst online.

1.2 Purpose

1.2.1 The purpose of this policy is to enable all individuals in our care who use the internet and social media at 3 Dimensions, to do so in a safe and responsible environment.

1.2.2 To understand the importance of reporting abuse, misuse or access to inappropriate materials and to know how to report it.

1.2.3 To ensure members of staff supervising individuals in our care on the internet or social media can:

- Ensure the online safety of individuals in our care.
- Have an effective approach to online safety, which protects and educate in the use of technology.
- Understand how to identify, intervene and escalate an incident, where appropriate.
- Understand what cyber bullying is and what its consequences can be
- Limit damage through the misuse of its I.T facilities.

1.2.4 This policy is based on the Department for Education's Statutory Safeguarding Guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

1.2.5 It reflects existing legislation, including but not limited to the Education Act 1996 the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on individuals' electronic devices where they believe there is a 'good reason' to do so.

1.3 Scope

1.3.1 This policy is communicated to all applicable people and organisations who have a responsibility for the online safety of individuals in our care and is also communicated to all individuals within our care.

1.3.2 All individuals who use or are responsible for those using IT equipment within

3 Dimensions, **must** adhere to this policy.

2 Policy Statement

2.1 Internet Access

2.1.1 Use of ICT facilities privileges may be revoked for inappropriate use including:

- Sending chain letters or spam emails
- Accessing files and folders which you have not been granted access
- Making unauthorised copies of data
- Destroying, deleting, erasing, or concealing data.
- Violating any UK laws or regulations in any way
- Engaging in unlawful or malicious activities
- Deliberately propagating any virus or malware
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages
- Sending, receiving, or accessing pornographic materials
- Defeating or attempting to defeat security restrictions on systems and applications.

2.1.2 We comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

2.1.3 If any member of staff is aware of any inappropriate activities involving any Individual in our care, they **must** immediately report this to the I.T Manager.

2.1.4 We have put in place appropriate filtering and monitoring safeguards, keeping individuals safe from potential harm online.

2.1.5 We ensure our ICT systems are secure and protected against viruses and malware, and such safety mechanisms are updated regularly

2.1.6 We conduct security checks and monitor the ICT systems on a weekly basis

2.1.7 We block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files

2.2 Privacy

2.2.1 We have the right to inspect all files stored on individual computers or storage media.

2.2.2 No one may access another person's computer files, or email without prior authorisation.

2.2.3 Individuals **must** assume whatever you do on 3 Dimensions computers is stored and subject to inspection at any time.

2.3 Email

2.3.1 If an individual in our care is sending emails, the account details **must** be registered with either the House or School Manager

2.3.2 Individuals **must** not share mailboxes to ensure clear monitoring of accounts

2.3.3 Individuals **must** not intentionally access Email accounts of others

2.3.4 Individuals **must** be aware email messages sent and received including web-based messaging are not private and are subject to viewing, downloading, and inspection

2.4 Personal Electronic Equipment

2.4.1 We manage the use of any type of camera phone, mobile phone camera, digital camera, or video camera in school and in the home.

2.4.2 Personally, owned equipment is not to be used without the permission.

3 Social Media

3.1.1 We understand social media can be a fun and rewarding way to share with family and friends around the world. However, use of social media also presents certain risks and carries with it certain responsibilities for members of staff to ensure the safety of individuals within our care.

Examples include

- Twitter
- Facebook
- YouTube
- Flickr
- Xbox Live
- Tumblr
- Pinterest
- Snapchat
- Instagram
- WhatsApp

3.1.2 You **must** be aware, information shared through social networking applications, even on private spaces, are still subject to copyright, Data Protection and Freedom of Information Legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislations.

3.2 Potential Risks of Using Social Networking

3.2.1 Most children and young people use the internet positively, but sometimes behave in ways that may place themselves at risk. Some risks do not

necessarily arise from the technology itself, but result from offline behaviours that are extended into the online world, and vice versa.

3.2.2 Potential risks can include:

- Bullying by peers and people considered ‘friends’
- Posting personal information that can identify and locate a child offline
- Sexual grooming, luring, exploitation and abuse contact with strangers
- Exposure to inappropriate images and/or content
- Involvement in making or distributing illegal or inappropriate content
- Theft of personal information
- Exposure to information and with others who encourage self-harm
- Exposure to racist or hate material
- Encouragement of violent behaviour
- Glorifying activities such as drug taking or excessive drinking
- Physical harm in making video footage, such as enacting and imitating stunts and risk-taking activities
- Leaving or running away from home because of contacts made online
- Of becoming a perpetrator.

4 Cyber-Bulling

4.1.1 To help prevent cyber-bullying, we ensure individuals understand what it is and what to do if you become aware of it happening to them or others.

4.1.2 We ensure individuals know how you can report any incidents and are encouraged to do so, including where you are a witness rather than the victim.

4.2 What is Cyber-Bullying?

4.2.1 Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

4.2.2 It can be an extension of face to- face bullying, with technology providing the bully with another route to harass their target.

4.2.3 However, it differs in several significant ways from other kinds of bullying:

- The invasion of home and personal space; the difficulty in controlling electronically circulated messages.
- the size of the audience.
- perceived anonymity

4.2.4 Cyber bullying includes the malicious use of:

- Mobile phones
- Instant messaging

- Chat rooms and message boards
- Video hosting sites such as YouTube
- Social network sites such as Facebook
- Webcams
- Virtual Learning Environments (VLEs)

4.2.5 Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise some incidents of cyberbullying are known to be unintentional and the result of simply not thinking about the consequences.

4.2.6 What may be sent as a joke, may not be received as one, and indeed the distance technology allows in communication means the sender may not see the impact of the message on the receiver.

4.2.7 In cyberbullying, bystanders can easily become perpetrators – by passing on or showing to other images designed to humiliate, for example, or by taking part in online polls or discussion groups

4.2.8 Individuals **mus**t be aware that their actions can have severe and distressing consequences.

4.3 Preventing and addressing cyber-bullying

4.3.1 We ensure individuals know how you can report any incidents and are encouraged to do so, including where you are a witness rather than the victim.

4.3.2 We actively discuss cyber-bullying, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

4.3.3 Staff are also encouraged to find opportunities to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

4.3.4 All staff receive training on cyber-bullying, its impact and ways to support individuals, as part of safeguarding training.

4.3.5 Where illegal, inappropriate or harmful material has been spread among individuals, we use all reasonable endeavours to ensure the incident is contained.

4.3.6 We take cyberbullying seriously. Individuals can be assured they will be supported when cyberbullying is reported.

4.3.7 We ensure that individuals in our care and staff are all aware of the procedures for dealing with cyberbullying, including bullying that takes place out of school or the home.

4.3.8 Strategies require continuous review and refinement as new technologies and services become popular.

4.3.9 All incidences of cyber bullying will be investigated and the investigation recorded and retained.

4.4 What to do with a report of cyber bullying:

- Reassure the person making the disclosure.
- Advise on how to prevent further instances and also how to keep the relevant evidence.
- Stop the circulation of the material.

4.4.1 When the bully has been identified, we will:

- Contact the parents/guardian of the bully and the victim.
- Contact the host site or phone company to make a report.

4.5 Examining electronic devices

4.5.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on individuals' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

4.5.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff **must** reasonably suspect the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break rules

4.5.3 If inappropriate material is found on the device, it is up to the staff member in conjunction with their relevant manager to decide whether they **must**:

- Delete material, or retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

4.5.4 Any searching of individuals will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

4.5.5 Any complaints about searching for or deleting inappropriate images or files on individuals' electronic devices will be dealt with through the school complaints procedure.

4.6 Signs and Symptoms

4.6.1 All staff **must** be aware of these possible signs which they **must** investigate when a child:

- is frightened of walking to or from school
- changes their usual routine
- is unwilling to go to school
- becomes withdrawn, anxious, or lacking in confidence
- begins to do poorly in school work
- has a desire to remain with adults
- Shows changes in their behaviour
- These signs and behaviours could indicate other problems, but bullying should be considered a possibility and **must** be investigated

4.7 Enforcement

4.7.1 This Policy is enforced by the I.T, Education and House Mangers.

The I.T Manager Ensures

- appropriate filtering and monitoring systems, which are updated on a regular basis
- ICT systems are secure and protected against viruses and malware, and such systems are updated regularly
- a full security check and monitoring of ICT systems on a weekly basis
- No access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- any online safety incidents are logged and dealt with appropriately
- Ensuring any incidents of cyber-bullying are dealt with appropriately

The Education and House Mangers Ensure

- staff understand this policy, and it is being implemented consistently.

4.7.2 Assessments are regularly carried out to monitor how well our policy and processes are working.

4.7.3 This is not to apply individual penalties associated with failing to comply with policy. Online Safety comes first, and this can only happen if:

- You are aware and happy with the procedure and systems in place
- You feel safe to report security incidents or mismanagement without worry of penalty

4.7.4 Intentional disregard of this policy unrelated to difficultly to understand or implement procedures may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

5 Practical Guidance for Young People

5.1 How to Deal with Cyber-Bullying

If Someone Spreads Rumours About You

5.1.1 If someone has posted false and malicious things about you on the internet or on a social networking site, it may be regarded as harassment. Harassment, on or off line, is a crime under UK laws.

5.1.2 This can be very distressing. Anything nasty posted about you can be seen by lots of people, very quickly, because it's so public and because the bullies make sure they tell everyone where to find the abuse.

5.1.3 Increasingly common are complaints that the spreading of malicious rumours and vicious gossip is being carried out by a person who was once your best friend.

5.1.4 So, chose your friends carefully. Be careful what you tell your friends. Keep your own secrets to yourself. Only tell people things if it wouldn't embarrass you if other people found out about it. Be cyber-savvy. Keep your own counsel.

If You Are Being Threatened

5.1.5 It's against the law in the UK to use the phone system - which includes the internet - to cause alarm or distress. It could even be against the 1997 Harassment Act.

5.1.6 If threats are made against you then it's essential that you alert someone you trust, or call a helpline or contact the Police. If someone is threatening you on the internet, or threatening someone you know, they could be committing a criminal offence.

5.1.7 Try to get documentary evidence if you can. By pressing the 'print screen' button, you should be able to print of a hard copy of the threatening text or images. Place it in a safe place, both on and off line.

5.1.8 If you need help doing this, call any helpline - as they should be able to talk you through it.

If You Are Being Groomed

5.1.9 Do not allow yourself to be intimidated into taking part in unacceptable behaviour over the internet, by someone on line who you do not know. Simply do not participate in something you feel uncomfortable about. Just refuse. Say NO!

5.1.10 These are not true friends. They are NOT the sort of people you want to be associated with.

5.1.11 They may even threaten you to say that if you do not do exactly what they

say, they will contact your family and/or friends and tell lies about you. They are unlikely to do this, this is just to frighten you into doing what they want you to do! Don't fall for it!

5.1.12 This behaviour is a serious criminal offence called "grooming". Men and women who have been found guilty of "grooming" have been sent to jail. You wouldn't get into a car with a stranger, would you? No! So, don't fall for this trick.

5.1.13 If you, or someone you know, is being groomed on-line by a stranger – report it immediately to someone you trust.

5.1.14 Do not hesitate to call an expert or report the matter to the Police. The Police are now able to get information from your computer's hard drive but it would be helpful if you did not delete anything that might be useful evidence of the grooming.

If Someone Posts Nasty Pictures of You

5.1.15 We all know how easy it is to snap a picture on a camera or mobile phone and then post it up on Facebook or on the internet.

5.1.16 Yes, isn't technology simply amazing. It is also a minefield of corruption and danger!

5.1.17 Make sure that you have a person's permission to take a picture of them for posting on-line, before you proceed. Once it has been posted thousands of people can see it on the internet. Don't offend others. Don't hurt someone you care about by uploading their picture, for others to have a laugh at. That could be considered harassment and harassment is against the law in the UK.

5.1.18 Don't digitally alter pictures of people either because what you might think is funny, may be offensive to other people.

5.1.19 Don't let anyone take a picture of you that might embarrass you.

5.2 Social Media Usage

Decide who will manage your social media

5.2.1 Decide who will be responsible for setting up, managing and moderating your social media accounts.

5.2.2 If you are using social media, talk to your School or House Manager to discuss this.

5.2.3 It is best managed by staff who are engaging with you while you are using the internet.

5.2.4 Before using the Internet or Social Media, staff & Carers will work with you to determine the appropriateness of using the Internet

Discuss the Rules of Using Social Media

5.2.5 Before setting up and using social media, staff and carers will discuss with you some of the expectation we and often the social media network has of you to follow when online.

These discussions **must** take place before any social media accounts are setup and used and **must** check you understand:

Online You Must:

- Be fair and courteous
- Always be honest and accurate when posting information or news, and if you make a mistake, correct it quickly
- Never post any information or rumours you know to be false
- Understand that the cyber world is the real world with real consequences.
- Keep in mind the internet or social media is not the appropriate place to resolve disagreements with people
- Keep in mind that any conduct that adversely affects people will not be tolerated
- Avoid posting complaints or criticism about other individuals as this could be viewed as malicious, obscene, threatening, or intimidating, or that might constitute harassment or bullying
- Remember that the Internet archives almost everything; therefore, even deleted posts can be searched.

5.2.6 Staff and carers will also discuss with you the importance of the following:

- You **must** not identify other young people at 3 Dimensions by name or post or publish information or images that may lead to their identification

5.3 Protect Your Privacy Online

5.3.1 You always need to protect your own privacy online.

5.3.2 Before using a social media account, make sure you look at the privacy and safety tools and the terms of service this will help you:

- Only display Information you wish to display
- Restrict who can contact you
- Restrict who can tag you in other social media posts

5.4 Think Before You Post

5.4.1 Posting online is instant, public and often, permanent. Once you post, you lose all control of what happens to it

5.4.2 It only takes one friend to share your content on their own profiles for it to be completely out of your hands.

5.4.3 Before you post content to social media sites, always take a moment to ask yourself these questions.

Why am I posting This?

- Is this something you really want to post?
- Does it really reflect your personality and values?
- Don't follow the crowd or post just to gain attention, as you might not like the response you get back.

Would I say this in person?

- No? Then you **must** not post it online

Would you be happy for your teacher, parent or carer to see it?

- No? Then you **must** not post it online

Can this be interpreted differently?

- Think about how others may take what you post
- Could it be offensive or inappropriate?

Is it private?

- Consider how many friends or followers you have. Can you trust each one of them not to share or talk about your posts with others?

What would you think of yourself?

- If you were a stranger looking in at your profile or posts, what would you think?
- If most of your posts are in some way critical, unkind, offensive or negative, how do you think you are being perceived?

Is it legal?

5.4.4 In the eyes of the law, posting online is not the same as having an informal chat with your friends. You are legally responsible for what you publish online

- Posting is publishing, just the same as if it was written in the newspaper.
- Even if your profile or message is private, you do not own what you publish - meaning anyone can use it as evidence.
- Make sure you do not post anything that might breach any UK or International law. Such as harassment, hate speech, threats of violence, ruining someone's reputation
- Pictures or comments suggesting or depicting illegal activity can all be

used against you.

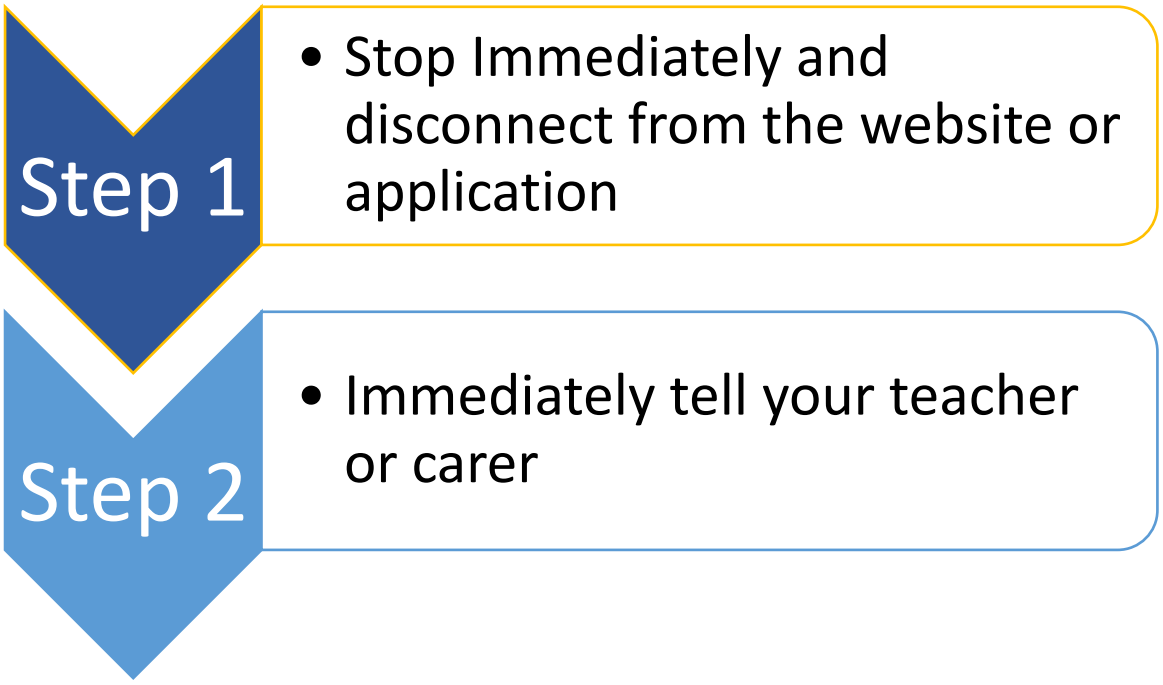
5.4.5 Inappropriate posts including discriminatory remarks, harassment, threats of violence or similar inappropriate or unlawful conduct will not be tolerated.

5.5 Report Abuse and Inappropriate Materials

5.5.1 If you believe you or someone else is the victim of cyber-bullying, you **must** speak to an adult as soon as possible. This person could be a carer, teacher, or the Education Manager/House Manager.

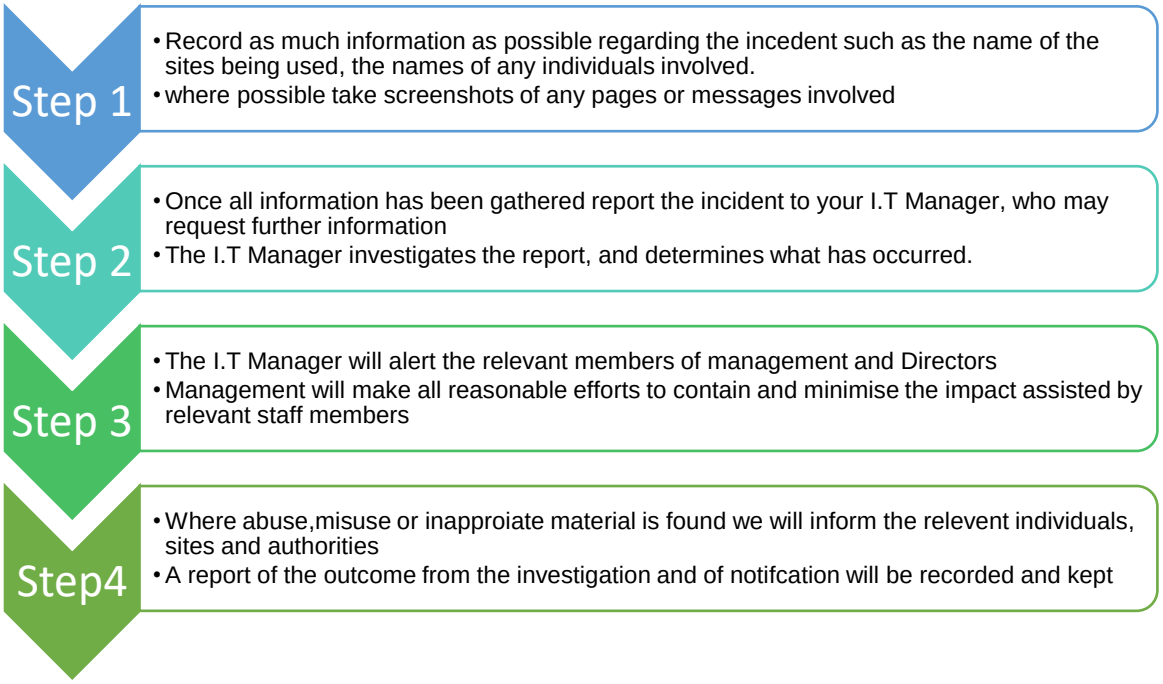
5.5.2 Do not delete anything until it has been shown to your Teacher, carer or the Education Manager/House Manager even if it is upsetting, the material is important evidence which may need to be used later as proof.

5.5.3 If you find yourself in a situation online where you feel, uncomfortable with the conversation, content or activity, you are to follow the steps below immediately



What Happens Next?

5.5.4 Your teacher or carer will need to collect some information regarding what has happened; the process they will follow is listed below:



6 Practical Guidance for Staff

6.1.1 All staff need to understand the way individuals communicate with others, and the potential risks. You need to know what the individuals are doing online and help them to do it in a safe way.

6.1.2 Asking them to simply not to use technology is not a realistic way to prevent or react to online safety issues.

6.1.3 With technology changing on a day-to-day basis, the best way to stay informed is to be involved.

6.1.4 If you suspect or are told about a cyber-bullying incident, follow the protocol outlined above:

6.2 Collecting Evidence from Individuals

6.2.1 When investigation incidences of online safety it is important to collect as much information as possible.

6.2.2 Following a report of cyberbullying or another online safety issue you **must** gather as much information as possible this may include accessing electronic equipment of the individual.

Mobile Phones

- Ask the individuals to show you the mobile phone, note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, record date, times and names.

- Tell the individual to save the message/image
- Go and see the Education Manager or House Manager, or in their absence, a Director.

6.2.3 Computers

- Ask the individual to get up on-screen the material in question.
- Ask the individual to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Taking the offending material, to see the Education Manager or House Manager.
- Any taken statements will then be followed up particularly if a child protection issue is presented.

6.3 Online Grooming and Sexual Exploitation

6.3.1 There is also concern the use of social networking services may increase the potential for sexual exploitation.

6.3.2 Exploitation can include exposure to harmful contents and encouragement for individuals to post inappropriate content or images of themselves.

6.3.3 There have also been many cases where people have used social networking as a means of grooming for sexual abuse.

6.3.4 The following are common tactics of online grooming:

- Gathering personal details, such as age, name, address, mobile number, name of school and photographs
- Promising meetings with celebrities or offers of merchandise
- Offering cheap tickets to sporting or music events
- Offering material gifts including electronic games, music or software
- Paying people to appear naked and perform sexual acts
- Bullying and intimidating behaviour, such as threatening to expose the individual or postings on a social networking site, and/or saying they know where they live, plays sport, or goes to school.
- Asking sexually themed questions, such as ‘Do you have a boyfriend?’ or ‘Are you a virgin?’
- Asking to meet offline
- Sending sexually themed images, depicting adult contents or the abuse
- Assuming a false identity on a social networking sites to deceive

Possible Indicators

A child may be experiencing abuse online if they:

- spend lots, much more or much less time online, texting, gaming or using social media
- are withdrawn, upset or outraged after using the internet or texting
- are secretive about who they're talking to and what they're doing online or on their mobile phone
- have lots of new phone numbers, texts or e-mail addresses on their mobile phone, laptop, computer or tablet.

Things you may notice

6.3.5 If you're worried an individual is being abused, watch out for any unusual behaviour such as:

- withdrawn
- suddenly behaves differently
- anxious
- clingy
- depressed
- aggressive
- problems sleeping
- eating disorders
- wets the bed
- soils clothes
- takes risks
- misses school
- changes in eating habits
- obsessive behaviour
- nightmares
- drugs
- alcohol
- self-harm
- thoughts about suicide