Fountaindale

Online E-Safety Policy

Sept 2017

Policy development

The online e-safety policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and Safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office

Roles and responsibilities

The school has an e-safety coordinator. Our coordinator is: Kelly Fedun

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devises.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon or the Hector Protector function.
- Issues such as Cyberbullying and online safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail form pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published
- The Principal or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the school website
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the County Council to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the Assistant Head-teacher responsible for new technologies and online e-safety or the ICT technician
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.

- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Videoconferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a videoconference call.
- Videoconferencing will use the educational broadband network to ensure quality of service and security

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents of pupils in the Formal curriculum will be asked to sign and return a consent form
- In the Pre-formal and Semi Formal Curriculums, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Formal pupils must apply for internet individually by agreeing to comply with the responsible internet use statement.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the online policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.

- Complaints of misuse by staff will be referred to the Principal
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the online safety policy.

Communicating the policy

Pupils

- Appropriate elements of the online safety policy will be shared with Formal pupils
- E-safety rules will be posted in all networked rooms
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified,

Staff

- All staff will be given a copy of the online e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting.

Parents

- Parents will be notified of the policy in newsletters, the school brochure and website
- Parents of Formal pupils will be asked to sign the parent/pupil agreement at the beginning of each academic year
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This Online E-Safety policy was revised by: Kelly Fedun

On (date): 9/9/2016

It was approved by the Governors on: ______________________________

Appendix 1
(Appendix 18 from the school's WHOLE SCHOOL POLICY FOR CHILD PROTECTION TO SAFEGUARD AND PROMOTE THE WELFARE OF CHILDREN September 2016 (Version 6 November 2016)

Online Safety

Our school ensures that children are able to use the internet and related communications technologies appropriately and safely and this is part of our wider duty of care. We recognise that the use of technology can be a significant component of many safeguarding issues including children sexual exploitation; radicalisation and sexual predation.

Online safety now covers the safety issues associated with all information systems and electronic communications as a whole. This encompasses not only the internet but all wireless electronic communications including mobile phones, games consoles, cameras and webcams. It also needs to take into account the increasing mobility of access to digital technology through the range of mobile devices.

Technology often provides a platform to facilitate harm. However, it important to remember that the issue at hand is not the technology but the behaviour around how it is used; the use of new technologies in education brings more benefits than risks.

Through our Online E-Safety Policy, our school will ensure that we meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside our school. The policy also forms part of our school's protection from legal challenge, relating to the use of digital technologies.

There are additional duties under the Counter terrorism and Securities Act 2015 which requires our school to ensure that children are safe from terrorist and extremist material on the internet.

Our school will ensure that there are filters and monitoring systems in place to limit exposure to risks when children are using the school's IT systems and technology that can be used online.

Our school recognises that whilst we have appropriate filters and monitoring systems in place, we also do not "over block" so that we do not restrict this teaching opportunity to teach children about keeping safe online.

Appendix 2
(Appendix 17 from the school's WHOLE SCHOOL POLICY FOR CHILD PROTECTION TO SAFEGUARD AND PROMOTE THE WELFARE OF CHILDREN September 2016 (Version 6 November 2016)

Youth Produced Sexual Imagery (Sexting)

Introduction

The school recognises that 'sexting' is a growing concern amongst professionals and parents as it can expose children to risks, particularly if the imagery is shared further. It can lead to embarrassment, bullying and increased vulnerability to sexual exploitation. Producing and sharing images of under-18's is also illegal.

There is no clear definition of what is 'sexting' and indeed many professionals, young people and parents have different interpretations ranging from sending flirty messages to sending nude or semi-nude photographs via mobiles or over the internet.

This guidance is based on the UKCCIS Sexting in Schools and Colleges guidance 2016. The full guidance is located at UKCCIS 2016 Guidance. This guidance 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

It does not cover:

- The sharing of sexual imagery of people under 18 by adults as this constitutes child sexual abuse and schools should always inform the police and CSC.
- Young people under the age of 18 sharing adult pornography or exchanging sexual texts which don't contain imagery.

The term youth produced sexual imagery has been adopted to provide some clarity and to distinguish it from imagery where there are adults involved in some manner.

The purpose of this guidance is to make expectations clear to pupils and their parents and carers as well as to be clear to staff about the school's policy and procedure in responding to incidents.

This policy forms part of our school's safeguarding arrangements and our response to concerns about 'sexting' will be guided by the principle of proportionality and our primary concern at all times is the welfare and protection of the children and young people involved.

The school recognises that it is an offence under the Sexual Offences Act 2003 to possess, distribute, show and make indecent images of children (a child being under 18 year) but it does not define what is indecent.

However the police accept that the law which criminalised indecent images of children was created before the technological advances of today and it originally sought to protect children from adults. It was not intended to criminalise children. Despite this children who share sexual imagery of themselves or peers are breaking the law and therefore we will seek to manage this type of case appropriately.

All professionals including the National Police Chiefs Council agree that incidents involving youth produced imagery should primarily be treated as a safeguarding issue. It is agreed that we should not unnecessarily criminalise children as the consequence of this can be significant in terms of their life chances in adulthood. Where children do share images it is often as a result of natural curiosity and exploring relationships and in the context of the digital world we live in.

The school is therefore empowered to deal with the majority of these incidents without involving the police.

Handling Incidents

The school may become aware of the issue in a variety of ways i.e. from the child direct, a friend of parent or a member of staff.

We recognise that the child is likely to be very embarrassed and worried about what might happen. We also recognise the pressure that is on a child can be under to take part in sharing such imagery but we will reassure them they are not on their own and will help and support them. We will also help them to understand what has happened and the context for the concerns. We will also discuss issues of consent and trust within healthy relationships.

All incidents will be followed in line with our safeguarding and child protection policy. Where an incident comes to our attention:

- The incident will be reported to the Designated Safeguarding Lead (DSL) as soon as possible.
- An initial meeting with the appropriate school staff will be held to:
    - Establish if there is immediate risk & what further information is needed, whether or not the imagery has been shared
    - Consider facts about the children involved which could influence a risk assessment. Further guidance and questions to consider is in Annexe A, page 31 UKCCIS Sexting in Schools Guidance 2016
- A meeting with the young person will be held (if appropriate)
- Parents will generally be informed at an early stage

An immediate referral to children’s social care and/or the police should be made if at the initial stage:

- The incident involves an adult
- The child has been coerced, blackmailed or groomed or if there are concerns about capacity to consent
- If the sexual acts are unusual for the developmental age or violent
- Children under 13 years are involved
- The child is at immediate risk e.g. suicidal or self-harming

Where the above do not apply then the school will generally deal with this matter without involving the police or children's social care although this will be subject to review.

This decision is made where we are confident that we have sufficient information to assess and manage any risks within our pastoral support and disciplinary framework. The decision will be made by the DSL with the input of the Head teacher and others as appropriate and will be recording.

Examples of cases where there is no need to involve the police are:

If a young person has shared imagery consensually, such as when in a romantic relationship, or as a joke, and there is no intended malice, it is usually appropriate for the school to manage the incident directly.

In contrast any incidents with aggravating factors, for example, a young person sharing someone else's imagery without consent and with malicious intent, should generally be referred to police and/or children's social care.

The following information will be considering when deciding on a course of action:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of the imagery?
- What is the impact on the young people involved?
- Do the young people involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?

Professional judgement will always be applied.

The images will not generally be viewed by staff unless there is a clear reason for doing so, reporting of the content is usually sufficient

- We will NOT copy, print or share the image as this is illegal

- If viewing is done, it will be with another member of safeguarding staff or senior leadership

Once a decision has been made not to involve the police or CSC then images may be deleted but we will be clear that this is appropriate action.

Where it is necessary to involve the police and it is appropriate we are authorised to seize any device (Education Act 2011) and pass it the police

CSC will be involved where are concerns which meet the threshold or if we know they are already involved with a child.

Case studies:

Case study A: Children and young people aged 13-18
Concern:

- *Two children, both aged 15, were in a relationship for the past month. The boy asked the girl for "sexy" pictures and she sent him a single topless photo. Afterwards the girl was worried that he might share the photo so she shared her concerns with her friends. Her friends then told their form tutor who spoke with the school DSL.*

School response:

- *The DSL spoke with the girl and then the boy. Both pupils confirmed there had not been any sexual activity between them. There were not any wider safeguarding concerns about either pupil. There was no evidence that the image had been shared by the boy and he offered to delete the image from his device.*
- *Both pupils were spoken with by the DSL who advised them on the potential impact of taking and sharing youth produced sexual imagery both criminally and emotionally. The DSL worked with both pupils to help them come up with an agreed plan to inform their parents. The school DSL documented the incident and as well as the actions taken in the children's safeguarding records.*

Case study B: Children aged under 13
Concern:

- *A class teacher found a naked photo of a child (boy, aged 11) on a school tablet. The child said that he had been using the tablet with two other children during lunchtime and they dared him to take a picture of his bottom.*

School response:

- *The school had no other safeguarding concerns about the children or their families. The school DSL spoke with the local authority education safeguarding team and subsequently accessed the local safeguarding board's guidance regarding underage sexual activity. This tool indicated that the behaviour was likely to be inappropriate but did not meet the threshold for a referral to children's social care.*
- *The school DSL spoke with the children involved and their parents and advised them on the situation and possible consequences including police and social care*

involvement. The children were sanctioned in school for their behaviour and the parents were fully supportive of the school's approach.

- *All members of staff were provided with updated online safety training and a reminder of the school online safety and acceptable use policy to ensure that children were not left unsupervised with school tablets. The school documented the incident and the actions taken in the children's safeguarding records.*

Educating Young People

As a school we need to teach children in an age appropriate way about youth produced imagery to prevent harm by providing them with the skills, attributes and knowledge to help them navigate risks.

This approach to tackling sensitive issues promotes a whole school approach to safeguarding giving children the space to explore key issues and the confidence to seek the support of adults should they encounter problems.

This issue will be taught as part of a wider PSHE programme and though IT curriculum work to underpin a specific message such as 'sexting'.

The work that we do therefore will include issues such as:

- communication
- understanding healthy relationships including trust
- understanding and respecting the concept of genuine consent
- understanding our rights (especially our collective right to *be* safe and to *feel* safe)
- recognising abusive and coercive language and behaviours
- accepting our responsibilities (especially our responsibility to respect others trust and protect their right to be physically, emotionally and reputationally safe)

Appendix 1

Helplines and reporting

- Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 11 11 or in an online chat at http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx.
- If parents or carers are concerned that their child is being contacted by adults as a result of having sharing sexual imagery they should report to NCA-CEOP at www.ceop.police.uk/safety-centre
- ChildLine and the Internet Watch Foundation have partnered to help children get sexual or naked images removed from the internet. Young person can get their photo removed by talking to a ChildLine counsellor. More information is available at http://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx
- If parents and carers are concerned about their child, they can contact the NSPCC Helpline by ringing 0808 800 5000, by emailing help@nspcc.org.uk, or

by texting 88858. They can also ring the Online Safety Helpline by ringing 0808 800 5002.

Advice and information for parents

- The NSPCC has information and advice about sexting available on its website: NSPCC Sexting
- The National Crime Agency/CEOP has produced a film resource for parents and carers to help them prevent their children coming to harm through sharing sexual imagery: THINKUKNOW Nude-selfies-a-parents-guide

- Childnet have information and advice about sexting available on its website: http://www.childnet.com/young-people/secondary/hot-topics/sexting

- Parent Info (http://parentinfo.org/) provides information and advice to parents from expert organisations on topics ranging from sex and relationships, mental health and online safety including sexting.

Resources parents could highlight to their children

- ChildLine have created Zip-It, an app that provides witty comebacks in order to help young person say no to requests for naked images Childline Zipit Ap
- There is information on the ChildLine website for young people about sexting: Childline information for young people
- The Safer Internet Centre has produced resources called 'Childnet So you got naked online which help young people to handle incidents of sexting

The NSPCC adults helpline: 0808 800 5002 The NSPCC has partnered with O2 to offer direct support to parents and other adults on issues relating to online safety.

ChildLine: www.childline.org.uk ChildLine offers direct support to children and young people including issues relating to the sharing of sexual imagery.

The Professionals Online Safety Helpline (POSH): http://www.saferinternet.org.uk/about/helpline Tel: 0844 381 4772. This helpline supports professionals with an online safety concern or an online safety concern for children in their care. Professionals are able to contact the helpline to resolve issues.

Resources for teaching staff

There is a wealth of resources for teachers at page 28 of the UKCCIS Sexting in Schools Guidance 2016

Appendix 3
NSCB Guidance (You must refer to following link for latest version http://nottinghamshirescb.proceduresonline.com/p_underage_abuse_ict.html in accordance with NSCB guidelines)

On-line Safety
RELATED GUIDANCE
See Local Practice Guidance, E Safety.
AMENDMENT
This chapter was updated in November 2016 to amend some of the terminology and clarify the on-line reporting process and additional link to a guide for parents whose children use social media has been added.

Contents

Further Information

1. Definition

'Internet Abuse' relates to five main areas of abuse of children:

- Indecent images of children (although these are not confined to the Internet);
- A child or young person being groomed online for the purpose of sexual abuse / exploitation;
- Exposure to pornographic or other offensive material on the Internet;
- Young people taking / sending indecent images of themselves (sexting);
- The use of the internet, and in particular social media, to engage children in extremist ideologies.

Internet abuse may also include cyber-bullying. This is when a child is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child using the Internet or mobile phones. It is essentially behaviour between children, although it is possible for one victim to be bullied by many perpetrators.

2. 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.

Social networking sites are often used by perpetrators as an easy way to access children and young people for sexual abuse. I

In addition 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, various paramilitary groups, extremist Animal Rights groups and others who justify political, religious, sexist or racist violence.

3. Indicators

Often these issues come to light through accidental discovery of images on a computer or other device and can seem to emerge 'out of the blue' from an otherwise trusted and non-suspicious individual. This in itself can make accepting the fact of the abuse difficult for those who know and may have trusted that individual.

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.

4. Protection

Where there is suspected or actual evidence of anyone accessing or creating indecent images of children, this must be referred to the Police and Children's Social Care Services.

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 Social Care Services.

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 under16 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 on just one occasion (previously it was on at least two occasions).

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 Social Care 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. Referrals will normally lead to a Strategy Discussion to determine the course of further investigation or enquiry. Intervention should be continually under review if further evidence comes to light. Professionals who are concerned about a child can contact the sexual exploitation investigation unit at Nottinghamshire Police.

The Sexual Exploitation Investigation Unit (SEIU) are part of Nottinghamshire Police's Public Protection. SEIU have primacy for investigations into Child Sexual Exploitation, Online grooming offences, Indecent Images of Children and Child Trafficking. SEIU are based at Holmes House at Mansfield but cover both the City and County Authorities and work closely with Children's Social Care.

Any information/intelligence or referral detail should be sent to the SEIU (Local Contacts) inbox.

Where there are concerns in relation to a child's exposure to extremist materials, the child's school may be able to provide advice and support: all schools are required to identify a Prevent Single Point of Contact (SPOC) who is the lead for safeguarding in relation to protecting individuals from radicalisation and involvement in terrorism.

Suspected online terrorist material can be reported through the Report online material promoting terrorism or extremism website. Content of concern can also be reported directly to social media platforms – see the UK Safer Internet Centre website.

5. 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.

Webcam abuse

How it happens:

- An abuser might pretend to be a boy or girl of the same age;
- They might even pretend to be someone they know;
- They chat and flirt online. They start to chat about sex;

- They ask for naked selfies, or to go naked on webcam; Then they threaten: “I will share this pic with everyone you know if you don’t do more things on webcam/ hurt yourself/ give me money... ”

Sexting
The “exchange of sexual messages or images” and “Creating, sharing and forwarding sexually suggestive nude or nearly nude images” through mobile phones and the internet.

Advice for young people

- Don’t do anything on webcam you wouldn’t want your friends or family to see;
- If they have already shared images;
- It is never too late to do anything;
- Report to CEOP using the RED Button;
- Tell someone you trust;
- Contact Childline for advice.

Appendix 3 Sexting in schools and colleges

Sexting in schools and colleges:

Responding to incidents and safeguarding young people

UKCCIS
UK COUNCIL FOR CHILD INTERNET SAFETY

This document is available at http://www.nottinghamshire.gov.uk/media/116038/sexting-in-schools.pdf