Conisbrough Ivanhoe Primary Academy

E-Safeguarding Policy

2017-18

This policy is linked with the Safeguarding Children Policy

Based on Model Policy created by Sue Spink, Brooke Primary School
October 2013 as recommended by DSCB

Contents

Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Ivanhoe Primary Academy*,* we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (including existing ones such as PCs, laptops, whiteboards, digital video equipment; and future resources including personal digital assistants (PDAs), tablets, webcams, voting systems, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As e-Safeguarding is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The school's Deputy Designated Safeguarding Officers, Mrs Wild and Miss Denigan, have been trained on ThinkUknow and CEOP, and most staff have been trained on e-safety by the Doncaster Safeguarding Children Board (DSCB) representative. It is the role of the Deputy Designated Safeguarding Officers to keep abreast of current issues and guidance through organisations such as the DfE, DSCB, Doncaster LA, other LAs, cybermentors, CEOP (Child Exploitation and Online Protection) and Childnet, and it is the role and responsibility of all staff to adhere to policy.

Senior Leadership and Governors are updated by the Head/ Deputy Designated Safeguarding Officers and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

Teaching and Support staff have a responsibility to read, understand and help promote the school's e-Safeguarding policy. They will endeavour to embed e-Safeguarding messages in learning activities across all areas of the curriculum. All staff will maintain a professional level of conduct in personal use of technology at all times.

All pupils have a responsibility to read, understand, and adhere to the school pupil Acceptable Use Policy. Pupils need to understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

Parents and carers have a responsibility to help and support the school in promoting e-Safeguarding. They should read and promote the school pupil Acceptable Use Agreement with their children. Parents will sign a home school agreement regarding safe use of ICT.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendix1&2), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE. The policy is updated annually and any issues are followed up with e-Safeguarding training.

Staff Training

- Staff should receive regular information on e-Safeguarding issues in the form of staff meetings and CPD, as appropriate.
- Staff will annually receive e-Safeguarding training.
- New staff (students, work experience placements and volunteers) will receive information on the school's Acceptable Use Policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart appendix 3).
- All staff are encouraged to incorporate e-Safeguarding activities and awareness within their curriculum areas.
- Governors sign a Social Networking Agreement (appendix 4).

Learning and Teaching

- At Ivanhoe, we endeavour to embed clear e-Safeguarding messages across the curriculum whenever the internet and related technologies are used.
- E-Safeguarding guidance should be given to the pupils on a regular and meaningful basis, and embedded within ICT opportunities throughout the curriculum.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safeguarding curriculum.
- Pupils should be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- The e-safeguarding policy will be introduced to the pupils at the start of each school year.
- E-safeguarding posters are prominently displayed in school shared areas.
- Children are made aware of how to access the alert button on CEOP.
- E-safeguarding rules are displayed in shared areas.
- Pupils and parents have access to E-safeguarding information.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Pupils are encouraged to keep their passwords secret and not to share with others.

- All users should read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safeguarding Policy.
- Adult users are provided with individual network and email details.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Subject Leader – Miss Huck.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Staff are encouraged to create passwords using a mixture of letters, numbers and symbols. Individual staff users must also make sure that workstations are not left unattended for long periods, this is protected by logins becoming locked after a short period of time.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published March 2009, available through YHGFL)

- Staff should be aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any ***school/ children/ pupil*** data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Corporate ICT DMBC filtering is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains that students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.

- If Internet research is set for homework, specific sites can be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work, as well as any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Infrastructure

- School internet access is controlled through the Local Authority.
- Ivanhoe Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Designated/Deputy Designated Safeguarding Officers and ICT Subject Leader.
- It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media (memory sticks, removable drives etc) are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility nor the network manager’s to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ICT Co-ordinator for a safety check, using the school’s virus scan first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT co-ordinator /Network Manager.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed immediately.

Managing other Web 2 technologies

Web 2, including social networking sites (eg Facebook), if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are taught to avoid placing images of themselves on such sites in school uniform with the school logo visible.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are.
- Our pupils should be advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils should be encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are taught to consider their digital footprint.
- Our pupils are asked to report any incidents of bullying to parents/ carers and the school.
- The school blog is managed by the Headteacher.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Members of staff should not contact a pupil or parent/ carer using their personal device.
- Pupils should not bring personal mobile devices/phones to school, unless previously agreed with the head teacher. If devices are accidentally brought into school, these must be handed in to the office.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate messaging between **any** member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school, schools or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account to use for all school business. School email accounts should be the only account that is used for school related business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure (see Password section). For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter may be written on school headed paper.
- Pupils are introduced to email as part of ICT in the curriculum.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

Managing Digital Content

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, can be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- The school permits the appropriate taking of images by staff and pupils with school equipment. Written consent of parents/carers for this is asked for when a child first enters school. This should be kept in the child's file, and a list kept by the class teacher which highlights those children who do not have consent.
- Staff should be discouraged in the use of personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips. However with the express permission of the Headteacher, images can be taken, provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Storage of Images

- Images/ films of children are stored on the school's network and should be deleted when those children leave the school.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

Webcams / Video Conferencing

- Webcams in school are only ever used for specific learning purposes, and should only be used in adult-led teaching situations.
- Misuse of the webcam by any member of the school community will result in sanctions as part of the school behaviour policy.
- Permission should be sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing
- Approval from the Headteacher is sought prior to all video conferences within school.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to e-Safeguarding should be made to the Designated/Deputy Designated Safeguarding Officers. Incidents should be logged, and kept in a central location.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Co-ordinator and Designated/Deputy Designated Safeguarding Leads.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Subject Leader and Designated/Deputy Designated Safeguarding Leads, and, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see attached flowchart,Appendix.)

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safeguarding rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safeguarding issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safeguarding. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safeguarding both in and outside of school. We aim to consult and discuss e-Safeguarding with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safeguarding policy
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-Safeguarding where appropriate in the form of;
    - Information evenings
    - Posters/leaflets
    - Website/ Blog postings
    - Newsletter items

Inclusion Statement

We believe that we are an educationally inclusive school where the teaching and learning, achievements, attitudes and well-being of every pupil matter.

Aims

We actively seek to remove the barriers to learning and participation that can hinder or exclude individual pupils, or groups of pupils. This means that equality of opportunity must be a reality for our children, regardless of race, gender and sex. We make this a reality through the attention we pay to the different individual and groups of children within our school to ensure minimal risk of underachievement.

The National Curriculum is a key part in planning a curriculum that meets the specific needs of individuals and groups of children. We meet these needs through:

- <u>Setting suitable learning challenges</u>
  – teachers teach knowledge, skills and understanding in ways that suit the pupil's abilities, including pupils whose attainments fall significantly below expected levels and pupils who exceed the expected level within one or more subjects.

- <u>Responding to children's diverse learning needs by</u>:
  - creating effective learning environments.
  - providing equality of opportunity.
  - securing their motivation and concentration.
  - using appropriate assessment approaches.
  - setting targets for learning.

- <u>Overcoming potential barriers to learning and assessment for individuals and groups of pupils</u>
  - helping with communication, language and literacy.
  - developing understanding
  - managing behaviour
  - managing emotions

This policy should be reviewed regularly, and take into account the ever-changing nature of the technologies involved.

K Wild

Deputy Head and Designated Safeguarding Lead

Next Review Date: July 2019

Appendix 1

Conisbrough Ivanhoe Primary Academy

Staff, Governor and Visitor
ICT Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Brian, Designated Safeguarding Officer, Mrs Wild or Miss Denigan, Deputy Designated Safeguarding Officers.

- I will only use the school's email / Internet / Intranet / and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on SIMS/EMAG) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Head teacher and Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safeguarding policy and help pupils to be safe and responsible in their use of ICT and related technologies.

School Equipment

- I accept that when school lap-tops, digital cameras etc. are taken home they must be covered by the householder’s home contents insurance policy.
- I understand that if it is necessary to leave school equipment in the car for a brief period, (not overnight,) it must be out of sight and the car must be locked. Otherwise the staff member will be liable for the full replacement costs as the item will not be covered by the school’s insurance.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……….……………………………………………………………..

Date ……………………

Full Name ……………………………………………………(printed)

Job title………………………………………………………………………

Appendix 2

Conisbrough Ivanhoe Primary Academy

Pupil Acceptable Use Agreement / e-Safeguarding Rules

Using the computers:

- I will only use ICT in school for school purposes.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not bring in cd's / memory sticks etc. from home and try to use them on the school system.

Using the internet:

- I will ask permission before using the internet.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I will not complete and send forms without permission from my teacher.
- I will not give my full name, home address or phone number when completing forms.

Using e-mail:

- I will ask permission before checking any email.
- I will only use my class email address when emailing,
- I will only email people I know or who my teacher has approved, and I will not open attachments.
- I understand that email messages I send or receive may be read by other people.
- I will immediately report any unpleasant messages sent to me.
- I will not give out my own details such as my name, phone number or home address.
- I will not use email to arrange to meet someone outside school hours.

Dear Parent/ Carer

ICT, including the internet, email and mobile technologies etc, has become an important part of learning in our school. We teach all children to be safe and responsible when using any ICT and expect them to follow e-safety rules.

As part of the school's ICT programme, we offer pupils supervised access to the internet. We believe that the use of the World Wide Web and E-mail is worthwhile and is an essential skill for children as they grow up in the modern world.

Before the school allows pupils to use the Internet, we seek parental permission. Please read and discuss the attached e-Safeguarding rules regarding safe use of ICT with your child and return the attached reply slip.

If you have any concerns or would like some explanation please contact school.

Yours Sincerely,

Head teacher

Consent for Internet Access and agreement to follow e-safety rules.

We give permission
for ……………………………………………………………………………………….
(child's name) to use the internet and e-mail in school.

We give permission for our child's work, if selected, to be published on the school web site.

We have discussed the e- Safeguarding rules and our child agrees to follow the e-Safeguarding rules and to support the safe use of ICT at Conisbrough Ivanhoe Primary Academy.

We understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.

We understand that the school cannot be held responsible for the nature or content of materials accessed through the internet.

We agree that the school is not liable for any damages arising from the use of the internet facilities.

Parent/ carer signature…………………………………………………………………

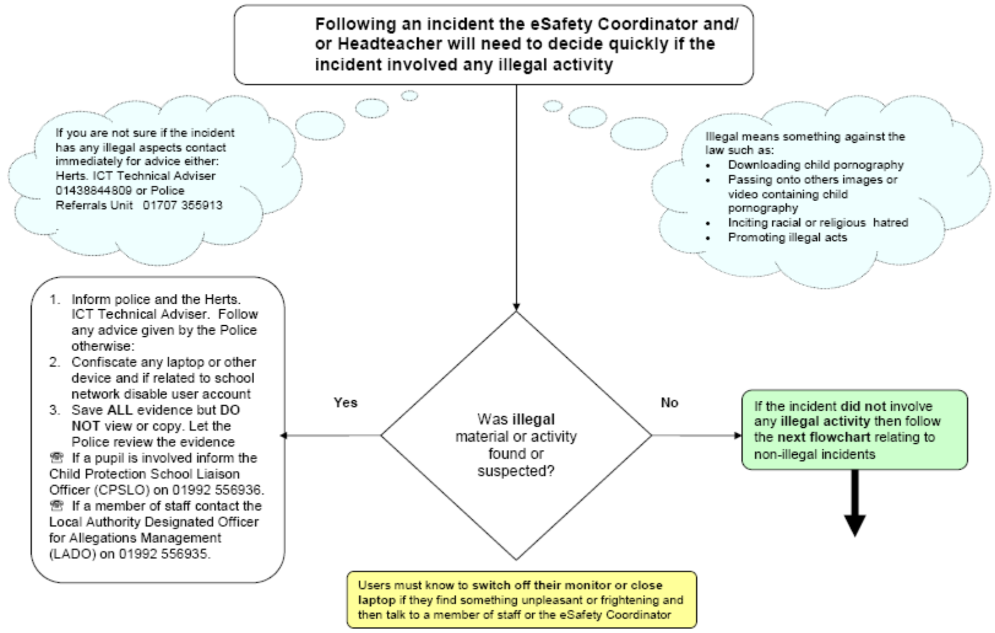
Full name…………………………………………………………………(printed)

Date………………………………………………………………………………….

Appendix 3

Flowcharts for Managing an e-Safety Incident

Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators



Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact immediately for advice either: Herts. ICT Technical Adviser 01438844809 or Police Referrals Unit 01707 355913

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Promoting illegal acts

Was **illegal** material or activity found or suspected?

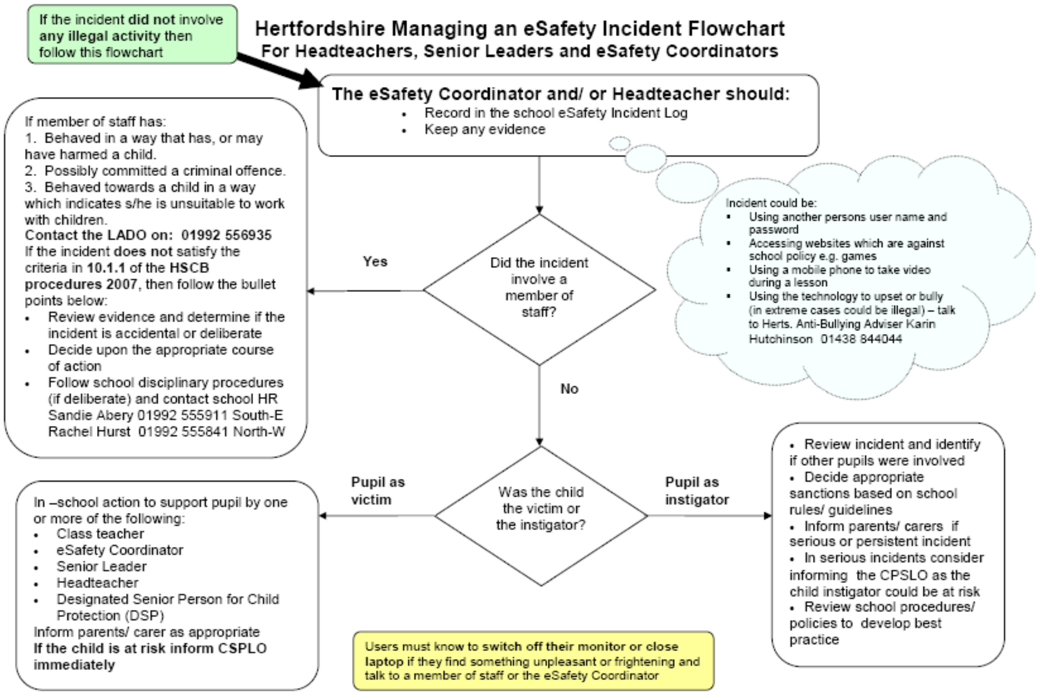
1. Inform police and the Herts. ICT Technical Adviser. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.

☎ If a member of staff contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 556935.

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to **switch off their monitor or close laptop** if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



If the incident **did not** involve **any illegal activity** then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart
For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:

- Using another persons user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844044

If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.
Contact the LADO on: 01992 556935
If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR Sandie Abery 01992 555911 South-E Rachel Hurst 01992 555841 North-W

In –school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader
- Headteacher
- Designated Senior Person for Child Protection (DSP)

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

Appendix 4

DONCASTER GOVERNORS' SUPPORT SERVICE

SOCIAL NETWORKING AGREEMENT

INTRODUCTION

Social Networking allows users to interact with one another in a virtual world. It is an online service, platform, or site that focuses on the building and reflecting of social networks or social relations between people.

A social network service consists of a group of people showing their social links. Most social network services are web based and provide means for users to interact over the internet, such as email and instant messaging. The main social networking site used is Facebook.

Governors should not:

- Refer to the school that you are a Governor at, or refer to any individual associated with that particular school in any way on a social networking site.
- Upload pictures of any individual without the consent of the individual/parent or guardian in the course of school business. To follow best practice, this should be avoided in both a professional and personal capacity.
- Become an on-line 'friend' with any student at the school.
- Upload any inappropriate/offensive language, images or comments on social networking site that may bring you and the school into disrepute. You should not publish anything that you do not want yourself and the school to be publicly associated with.

I, ____

a Governor at ____ agree to adhere to the above statements in my role as Governor and understand that if I were to undertake any of the unadvisable actions this may lead to suspension and/or removal from the Governing Body.

Signed: ____

Print: ____

Date: ____

Prepared on behalf of the Governors' Support Service
By Doncaster Council's eLearning Team

Current Legislation regarding e-safeguarding

Acts relating to monitoring of staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafeguarding

Racial and Religious Hatred Act 2006
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.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
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.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
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.

Protection of Children Act 1978 (Section 1)
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.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

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.