St Hugh's School

E-Safety Policy

Contents

1. Introduction

This policy has been formulated to support the school safeguarding policy. It covers all areas of safeguarding related to digital devices and the internet. It was produced using the following guidance.

> *"Sexting in schools and colleges: Responding to incidents and safeguarding young people" UK Council for Child Internet Safety. September 2016*
> "Keeping children safe in education Statutory guidance for schools and Colleges" *Department for Education – September 2016*

2. Aim

The aim of this policy is to provide guidance for the prevention of and management of E-Safety incidents within school. It is a complimentary document to the Safeguarding policy. It covers education, training, monitoring as well as methods for dealing with specific issues.

3. Definitions

E-Safety – Knowledge and understanding of risks on the internet or other online areas and an understanding of how to manage these risks.

Social Media -Websites and applications that enable users to create and share content or to participate in social networking.1

Sexting - Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. [2]

YPSI – Youngsters Preparing Sexual Imagery – Taking and distributing photographs by students under 18 years old. [3]

Pornography - Printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.[4]

DSO – Designated Safeguarding Officer

4. Roles and Responsibilities

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the E-Safety Co-coordinator and DSO
- The Head Teacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant

[1] OED https://en.oxforddictionaries.com/definition/social_media
[2] NSPCC https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/
[3] UKCCIS https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF
[4] OED https://en.oxforddictionaries.com/definition/pornography

- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership will receive regular monitoring reports from the E-Safety Coordinator/ICT Subject Leader and included in the termly report to governors
- The Head Teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff

E-Safety Coordinator/ICT Subject Leader

- Leads on e-Safety
- Takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- Provides training and advice for staff
- Liaises with Network manager
- Produces and receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments
- Meets regularly with DSO to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team and governors
- Updates policy
- Monitors staff training
- Logs audit results

School Network Manager

These staff are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the school's networks through a properly enforced password protection policy
- The school's filtering policy is applied and updated on a regular basis
- That he / she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- That monitoring software / systems are implemented and updated as agreed in school policies
- That school mobile devices are monitored for content

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the appropriate person for investigation

- Digital communications with students / Students (e-mail / Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school communication systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school e-Safety and Acceptable Use Policy
- Students have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where Internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches
- Reporting any CP issues immediately to a designated officer
- Follow the school guidance on Social Media use

Designated Senior Officers for child protection

Staff should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- Have an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand, at an appropriate level, school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school
- Should interact with E-Safety activities in school

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy

- Accessing the school website / VLE / on-line student / Student records in accordance with the relevant school Acceptable Use Policy.

5. Policy Statements

Education – Students

- A planned e-Safety programme should be provided as part of Computing lessons assessed with the BSquared system. It should be included in all other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and beyond school
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities including whole school theme days
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in all rooms
- Displays will be made around school to encourage safe internet use
- Staff should act as good role models in their use of ICT, the Internet and mobile devices
- Annual audits of student's understanding to inform planning

Education & Training – Staff

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff
- An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies
- There will be an annual update staff meeting on E-Safety as well as whenever new legislation is introduced
- Staff are expected to keep themselves informed to the latest developments in E-safety and technology

Network Manager

School network manager will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (and Head of Computing) must also be available to the Head Teacher or other nominated senior leader
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school has provided appropriate user-level filtering through the use of the Smoothwall filtering programme
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher (or other nominated senior leader). Requests from staff for sites to be added or removed from the filtered list will be actioned by the Network Manager
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users activity
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data [5]
- An agreed policy is in place with time limited passwords for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system
- Settings within the server forbids staff from installing programmes on school workstations / portable devices
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable device[6]
- The school infrastructure and individual workstations are protected by up to date virus software (Sophos as recommended by YHGFL)
- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured[7]

Use of images

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites
- Staff are allowed to take and use images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking images that students are not participating in activities that put them at risk or bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission

[5] See individual policy
[6] See Information Security Policy
[7] See Information Security Policy for further details

- Photographs published on the website, or elsewhere that include students must have written permission from parents / carers to be used.
- Students' full names will not be used anywhere on a website or blog,
- No names should ever be used in association with photographs
- Student's work can only be published with the permission of the
- Student and parents / carers

Email

There are responsibilities involved in using e-mail. In signing the School Acceptable Use Policy all employees agree to fulfil these responsibilities and acknowledge the wider LA Policy and UK Data Protection law.

- All School staff are allocated a "@st-hughs.n-lincs.sch.uk" e-mail address when they join the School. This e-mail address should be used for all official e-mails. The use of a private e-mail address to send and receive school emails is forbidden
- All administration staff will be also given a North Lincolnshire E-Mail address

General Considerations when using E-mail:

- E-mail is not a confidential means of communication. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and in particular recognise that e-mails can be:
    - Intercepted by third parties (legally or otherwise)
    - Wrongly addressed
    - Forwarded accidentally
    - Forwarded by initial recipients to third parties against your wishes
    - Viewed accidentally on recipients' computer screens
- Sensitive personal data should not be communicated by e-mail
- Staff must not include any defamatory comments in any e-mail messages
- Email is a form of publication and the laws relating to defamation apply. A comment made in jest can be misinterpreted by its recipient. In – for example - a case of harassment it is the effect of a communication which is considered and not the intention of the sender
- Staff must never use a false identity in e-mails, and must be aware that there is no guarantee that e-mail received was in fact sent by the purported sender. If, for any reason, an e-mail is sent on behalf of someone else the sender must make that clear at the beginning of the message
- The school e-mail system must not be used to create or distribute unsolicited, offensive, or unwanted e-mail, including the dissemination of chain letters. The sending of unsolicited marketing messages is now a criminal offence
- Email messages can be monitored by the Network Manager
- E-mail messages that show St Hugh's in an unprofessional light or that could expose St Hugh's to legal liability must not be sent by any member of staff. E-mails sent by a member of St Hugh's have the same standing as a letter on headed notepaper even if the contents are described as "private"
- Be very careful when downloading material from the internet and opening external e-mails if there is any suspicion of it including a virus. If you have any suspicions, do not open an attachment and contact your school ICT staff
- Staff must not invade anyone's privacy by any means using e-mail
- E-mail is not a substitute for record-keeping purposes. Where long term accessibility is an issue staff must transfer e-mail records to a more lasting medium or other electronic environment

- The laws applying to copyright apply to e-mail messages and attachments
- Documents attached to e-mails may contain information from which the history of a document's creation may be deduced. This data may identify those involved in generating or altering that item
- As a member of St Hugh's staff you are covered by the Data Protection Act (1998). This prescribes a number of further rights and responsibilities in using e-mail
- Personal data is subject to the Act. Under its terms, personal data includes any information about a living identifiable individual, including his/her name, address, phone number, and e-mail address. If you include such information in an e-mail or an attachment to an e-mail, you are deemed to be "processing" personal data and must abide by the Act. Personal information includes any expression of opinion
- Putting personal information (and especially personal sensitive information) in an unencrypted e-mail bears significant risk and is not an acceptable practice.
- St Hugh's has by law to provide any personal information held about any data subject who requests it under the Act. This includes information on individual PCs in departments and all staff have a responsibility to comply with any instruction to release such data made by St Hugh's Data Protection Lead. E-mails which contain personal information and are held in live, archive or back-up systems or have been "deleted" from the live systems, but are still capable of recovery, may be accessible by data subjects
- The law also imposes rules on the retention of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected

Social Networks

- Social networking applications include, but are not limited to:
    1. Social Networks (e.g. Facebook)
    2. Bookmarking sites (e.g StumbleUpon)
    3. Social News (E.g Reddit)
    4. Media Sharing (e.g Youtube)
    5. Microblogging (e.g. Twitter)
    6. Blog Comments and Forums [8]
- Staff and students must not access social networking sites for personal use via school information systems, school networks or using school equipment
- If staff access social networking sites using their personal computer systems and equipment, they should never give out personal information of any kind which could identify themselves, colleagues and / or pupils as staff at St Hugh's
- Staff must not place inappropriate photographs on any social network space and must – where they do post photographs - ensure that background detail (eg house number, street name, school) cannot identify them
- No photographs are to be posted of school activities or within the school grounds unless through the official school Social Media accounts
- Staff are not to communicate or "friend" students within the school
- Former students and parents of students are to only be added after notifying the Head teacher or other member of the Senior Leadership Team
- All parents and student's currently "Friended" on social media must be removed on signing of this policy unless exemption given by the Head teacher
- Staff must not run social network spaces for student use on a personal basis
- Schools are vulnerable to material posted about them online and all staff should be made aware of the need to report this should they become aware of anything bringing the

[8] http://timgrahl.com/the-6-types-of-social-media/

school into disrepute. Schools are advised to check regularly, using a search engine, to see if any such material has been posted

- If staff use social networking sites they should not publish specific and detailed "personal views" relating to the Agency, its schools, staff or students.
- Breaches of these regulations will lead to disciplinary action[9]
- The school network and IT facilities must not be used for the following activities:
  - Conducting illegal activities
  - Accessing or downloading pornographic material
  - Gambling
  - Soliciting for personal gain or profit
  - Managing or providing a business or service
  - Revealing or publicising proprietary or confidential information
  - Representing personal opinions as those of the Agency or its schools
  - Making or posting indecent or offensive remarks or proposals

Reporting Process for E-Safety Incidents

The following process is for reporting E-Safety incidents. It is important that all reports are made in a timely manner and all incidents to be treat seriously.

On discovery of an E-Safety issue staff are to immediately complete a white concern slip and pass to a DSO.

They will then investigate further and involve the E-Safety Officer and other agencies as necessary. Parent's / Carer's will be notified if appropriate.

The Network manager will be notified of any changes needed to the systems.

The documentation will then be recorded as necessary on Safeguarding documentation. The Child will be added to the monthly concerns sheet at an appropriate level.

Legislation

The following legislation - enforceable against public sector employees including school staff - must be considered when using the internet or email:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)3
- Data Protection Act 1998
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988, amended by the Copyright and Related Rights Regulations 2003
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988
- 2010 Equalities Act

[9] See separate policy for more details.

These Acts are concerned with material that might be

- criminal,
- cause harm to young people or
- be otherwise unlawful.

Enforcement

- Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible School employee being suspended.
- The school reserves the right to require the closure of any applications or removal of content published by Agency representatives which may adversely affect the reputation of St Hugh's or put it at risk of legal action.

Guidance on PCSI

Introduction

PCSI in school should be handled in the same way with a few exceptions due to the visual nature of the images.

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

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if
- appropriate)
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately[10]

Initial Review Meeting

The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or
- platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from
- devices or online services
- Any relevant facts about the young people involved which would influence
- risk assessment

[10] Sexting in Schools https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care 16/LADO should be made if at this initial stage:

- The incident involves an adult/member of staff
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
- What you know about the imagery suggests the content depicts sexual acts
- which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the imagery is under 1317
- You have reason to believe a pupil or pupil is at immediate risk of harm owing
- to the sharing of the imagery, for example, the young person is presenting as
- suicidal or self-harming

If none of the above apply then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light). The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSO is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.[11]

Searching devices, viewing and deleting imagery

Viewing the imagery:

- Adults should not view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSOs have been told about the content of the imagery
- The decision to view imagery should be based on the professional judgement of the DSO and should always comply with the child protection policy and procedures of the school or college. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil
- If a decision is made to view imagery the DSO would need to be satisfied that viewing:
    - is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
    - is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
    - is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network

If it is necessary to view the imagery then the DSO should:

- Never copy, print or share the imagery; this is illegal
- Discuss the decision with the Head Teacher
- Ensure viewing is undertaken by the DSO or another member of the safeguarding team with delegated authority from the Head Teacher

[11] Sexting in school https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

- Ensure viewing takes place with another member of staff present in the room, ideally the Head Teacher or a member of the senior leadership team. This staff member does not need to view the images
- Wherever possible ensure viewing takes place on school or college premises, ideally in the Head Teacher or a member of the senior leadership team's office
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery
- Record the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions Ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents

Appendix 1 – Staff Code of Conduct
Appendix 2 – Student Code of Conduct
Appendix 3 – Record of E-Safety Training

Author – Stuart Pattison 16/9/16