Horizon Academy Trust

Where anything is possible

Online Safety Policy

Approved by the Governing Body:	Autumn 2017
Term policy produced:	Autumn 2017
Date of next review:	Autumn 2019

INTRODUCTION

Our Online Safety Policy has been written, following government guidance. It has been agreed by all staff and approved by governors.

The Online Safety Policy and its implementation will be reviewed annually, or when changes are necessary to comply with school policy or national legislation.

Online Safety Officers have been identified in each school:

Cleeve Academy – Mrs Teresa Knight
Biggin Hill Primary Academy– Mr Stuart Clark

The schools have appointed a member of the governing body to take lead responsibility for online-safety:

Cleeve Academy – Mr Stuart Clark
Biggin Hill Primary Academy – Mrs Kath Cutler

EFFECTIVE PRACTICE

Online safeguarding depends on effective practice at a number of levels.

- Responsible ICT use by all staff and students; encourage by education and made explicit through published policies.
- Sound implementation of e-safeguarding policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Kingston Communications
- Effective management of filtering through the Smoothwall system
- National Education Network standards and specifications.

TEACHING AND LEARNING

- We will provide a curriculum/PSHE curriculum/other lessons which has e-safeguarding related lessons embedded throughout.
- Pupils will be taught how to use a range of age appropriate online tools in a safe and effective way.
- The academy will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Staff will model safe and responsible behaviour in their own use of technology during lesson.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be made aware of where to seek advice or help if they are experiencing problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

STAFF TRAINING

All staff receives training on online safety issues with updates as and when new issues arise in the form of staff insets.

- As part of the induction process all new staff receive information and guidance on the online safety policy, the schools acceptable use policies, data protection policy and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff should be aware of the indicators of abused/neglected including online.
- All staff understands that online bullying can result in emotional abuse.
- All staff knows that sexual abuse can occur via the internet and involve a range of activities.
- Staff should have an awareness of youth produced sexual imagery (sexting) peer on peer.
- Staff should know how to respond to 'sexting' concerns appropriately.
- Be aware sexual harassment can take place online as well as off line.
- Be aware the internet can play a role in gang activity.

MANAGING SYSTEMS

SECURITY/MONITORING/FILTERING

- Virus protection is installed on all hardware and will be kept updated regularly**.**

- Servers and other infrastructure will be located securely with only named appropriate staff permitted access.

- School will be responsible for ensuring that access to computer systems is as safe and secure as reasonably possible.

- It is the schools responsibility to ensure the Wi-Fi system has to levels of security:

  1. One giving suitable access to the schools network system. This has to be used with a secure password which is only given to key people.
  2. A second higher level security for visitors, guests and personable mobile devices. This has to be used with a second password that gives limited access and monitors the IP address/mac address of any device, making it traceable.

- Monitoring activity is in place through smoothwall. Any suspicious activity is reported directly from smoothwall via email alerts to the online safety officer. These reports are investigated quickly.

- The use of computer systems without permission or for inappropriate purposes could constitute criminal offence under the Computer Misuse Act 1990 and breaches will be reported the appropriate authorities.

- Filtering is managed in house. A risk assessment will be done when requests are brought to open websites and closed as soon as possible after use, the Head teacher should approve before opening.

E-MAIL

- Staff will only use official school provided email accounts to communicate with pupils/parents and carers.
- Staff should not access personal email accounts during school hours or for professional purposes, especially to exchange any school related information or documentation.
- The secure email system should be used at all times to send sensitive data outside the school system.
- Pupils and staff will be allocated an email account for use in school.
- Pupils must immediately tell a teachers or trusted adult if they receive any inappropriate or offensive emails.

PUBLISHING PUPILS IMAGES AND WORK

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Any images, videos of pupils must be stored on the school network and never transferred to personally – owned equipment.
- The school will store images of pupils that have left the school for 2 years following their departure for use in school activities and promotional resources.
- The online safety officer or technician is responsible for deleting the images off the network when they are no longer required or the pupils have left the school.

PUBLISHING STAFF IMAGES

- Consent will be sought from all staff before their images are posted online or used in any publications.
- Staff have the right to withdraw consent at all times.
- Images that are stored on the school server or the school website will be deleted no later than a month after the member of staff leave the school.

SOCIAL NETWORKING

- Staff will not post inappropriate content or participate in any conversations which will be damaging to the school. Staff who hold an account should not have pupils (past or present under 18 years of age) as their ‘friends’ unless the account has been specifically opened for professional use e.g. home school links. Doing so will result in disciplinary action or dismissal. Please see guidance for professionals working with young people document.
- School blogs/podcasts or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team/Senior manager. Employees/Volunteers should be advised not to run social network spaces for children and young people’s use on a personal basis.
- Social networking sites are blocked in school with exception of Twitter/Facebook which gives staff the ability to contribute to the school account. This is monitored by Sharon Carmichael (Family Links) and Sam Pinder (HLTA).

MANAGING EMERGING TECHNOLOGIES, MOBILE PHONES AND DEVICES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.

Mobile Phones and Devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos will be taken on mobile phones or personally-owned devices. Photographs and recordings can only be transferred from a school device to and stored on a school computer before printing.
- In the case of school productions, Parents/carers are permitted to take photographs of their own child in accordance with school protocols which strongly advise against the publication of any such photographs on Social networking sites.
- There are school mobile phones which are to be used when on school trips for communication/emergencies.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils’ use of personal devices

- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils will be provided with school iPods/iPads to use in specific learning activities under the supervision of a member of staff. Such mobile devices will be set up so that only those features required for the activity will be enabled.

Staffs’ use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Mobile Phones and personally-owned devices will be switched off or switched to ‘silent’ mode, Bluetooth communication should be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- The above is with exception to the caretaker who uses a personal mobile phone to arrange contractors, photograph health and safety issues on site and in emergencies contacts parents. This has been directed by the Head of School.

DATA PROTECTION AND INFORMATION SECURITY

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Any access to personal and sensitive information should be assessed and granted by the SIRO (Head of School) and the applicable IAO (-Business manager)
- For visitors using their own device; they will be given a unique code to access the Wi-Fi. This allows the school to identify the user if needed.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.

- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.

FAILURE TO COMPLY

Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff and may result in disciplinary action being taken.

RESPONSE TO AN INCIDENT OF CONCERN

An important element of online safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report online-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents on the secure electronic reporting system CPOMs. All staff has restricted access to the system with the ability to report any online/safeguarding issue any time. Key members of staff hold full access keys which gives them the ability to respond to and analyse incidents. The chain below demonstrates the key members of staff for which a cause for concern is dealt with in school.

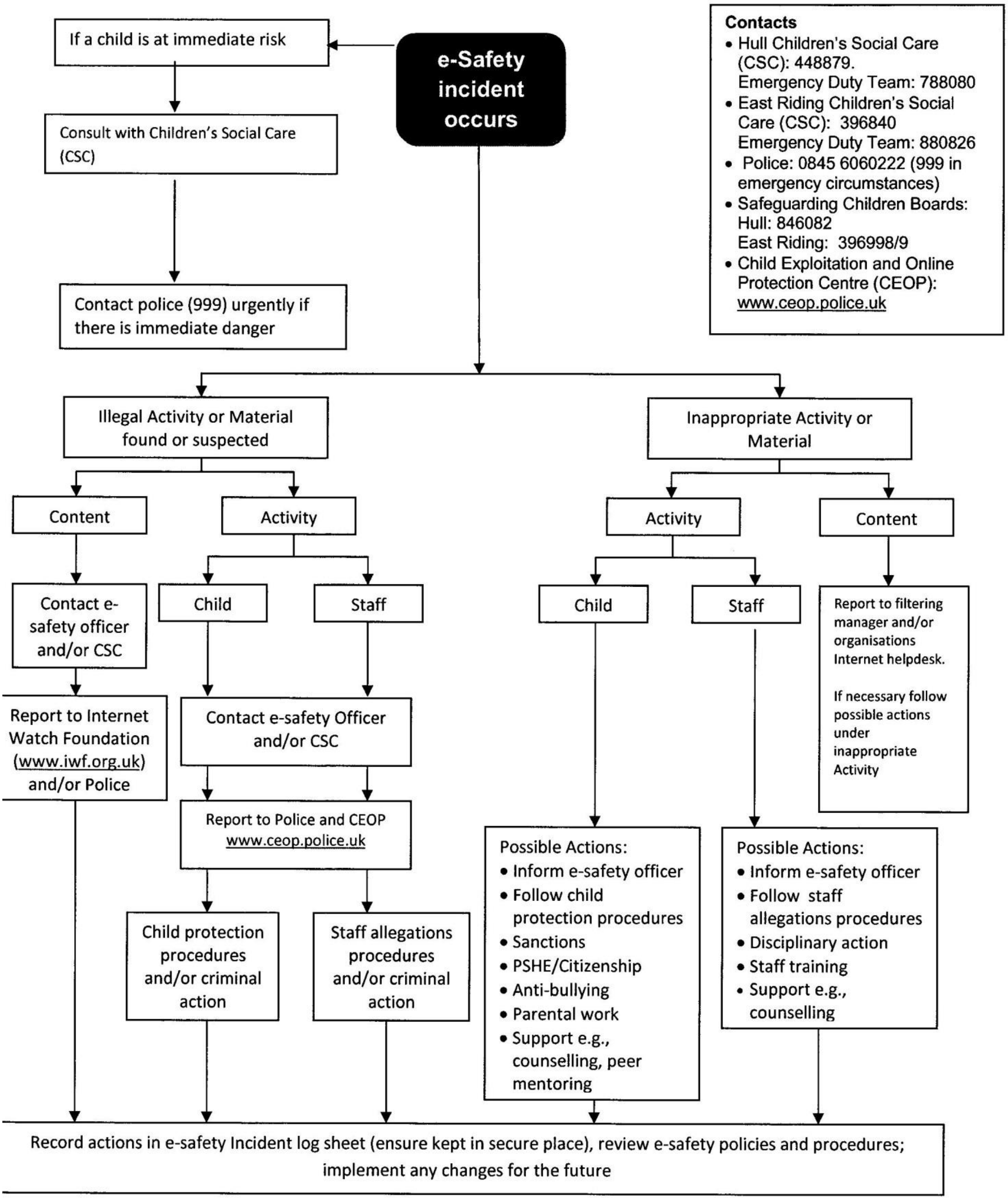
Online safety Officer
Mr Stuart Clark

Safeguarding Officer
Miss Rachael Harraway

Behaviour Co-ordinator
Mrs Catherine Simpson

2.4.9 Response to Risk Flowchart

Response to and Reporting of an e-Safety Incident of Concern



Contacts

- Hull Children's Social Care (CSC): 448879.
  Emergency Duty Team: 788080
- East Riding Children's Social Care (CSC): 396840
  Emergency Duty Team: 880826
- Police: 0845 6060222 (999 in emergency circumstances)
- Safeguarding Children Boards:
  Hull: 846082
  East Riding: 396998/9
- Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk

e-Safety incident occurs

If a child is at immediate risk

Consult with Children's Social Care (CSC)

Contact police (999) urgently if there is immediate danger

Illegal Activity or Material found or suspected

Content

Contact e-safety officer and/or CSC

Report to Internet Watch Foundation (www.iwf.org.uk) and/or Police

Activity

Child

Staff

Contact e-safety Officer and/or CSC

Report to Police and CEOP www.ceop.police.uk

Child protection procedures and/or criminal action

Staff allegations procedures and/or criminal action

Inappropriate Activity or Material

Activity

Child

Possible Actions:
- Inform e-safety officer
- Follow child protection procedures
- Sanctions
- PSHE/Citizenship
- Anti-bullying
- Parental work
- Support e.g., counselling, peer mentoring

Staff

Possible Actions:
- Inform e-safety officer
- Follow staff allegations procedures
- Disciplinary action
- Staff training
- Support e.g., counselling

Content

Report to filtering manager and/or organisations Internet helpdesk.

If necessary follow possible actions under inappropriate Activity

Record actions in e-safety Incident log sheet (ensure kept in secure place), review e-safety policies and procedures; implement any changes for the future

ACCEPTABLE INTERNET USE STATEMENT FOR ALL SCHOOL STAFF

Technology is provided and maintained for the benefit of all staff within Horizon to enhance skills and become more effective in the workplace. You are encouraged to use and enjoy these resources, using the following agreement as a guide.

There is a need to ensure that digital technologies are used appropriately and for you to have an understanding of your responsibilities in keeping yourself and young people safe. This guide aims to assist you, making sure that you have all necessary measures in place.

Internet and Email:

- I agree to only access suitable material;

  I am aware that accessing materials which are unlawful, obscene or abusive is not permitted.
- I agree to report unsuitable material;

  If I receive an email containing material of a violent, dangerous, racist, or inappropriate content, I will always report such messages to the Online-safety Co-ordinator.
- I agree to the professional code of behaviour;

  I appreciate that other users might have different views from my own and acknowledge that the use of strong language or aggressive behaviour is not acceptable.
- I agree to keep within copyright laws;

  I will respect work and ownership rights of people, including abiding by copyright laws.
- I agree to the responsible use of social networks, both within and outside the workplace;

  The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.

Equipment:

- I agree to take care to protect hardware and software;

  This includes protecting the ICT equipment from spillages by eating or drinking well away from them. I will always get permission before installing, attempting to install or storing programs of any type on the ICT equipment. I will always check files brought in on removable media (such as CDs, flash drives etc) and mobile equipment with antivirus software and only use them if they are found to be clean of viruses. I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could damage files or software. I will only transport sensitive data on encrypted removable media (laptops, USB sticks etc).
- I agree to only using equipment within the context of my professional role;

  I will only use ICT equipment for Horizon Trust purposes. I understand that activities such as buying or selling goods are inappropriate.

Security and Privacy:

- I agree to take measures to protect access to data;

  I will keep my log-on user name and password private, always log off when I have finished working or am leaving the ICT equipment unattended and regularly change my password (minimum of every 3 months). I am aware that I must never use someone else's user name. To protect myself and the systems, I will respect the security on the ICT equipment; I understand that attempting to bypass or alter the settings may put my work or other people's information at risk. I will not send sensitive information via FAX or non-secure email.

Mobile phones:

- I agree to always abide by Horizon Trust policy for use of mobiles in the workplace;

  I understand that the use of mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of my line manager and recorded.

Name (print)…………………………………………………………………….

Signed………………………..…………………………………………………….

Organisation…………………………………….……………………………

Date…………………………………….……………………………………..

Acceptable Use Policy - Early Years and KS1

As part of pupil's curriculum enhancement and development of ICT skills, Horizon is providing supervised access to the internet including emails.

Our internet access has a built in filtering system that restricts access to sites containing inappropriate content. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

Action
Read this with your child, sign it and return it to school.

I agree I will:

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed Parent/Carer ………………………………….. Date ………………..

Name of Child…………………………....... Class………………….

Acceptable Usage Policy KS2 Children

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, netbooks, and everything else including cameras and other devices. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

- At all times, I will think before I click
- When using the internet, I will think about the websites I am accessing
  If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I will think before deleting files
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed

Signed (Pupil) ____________________ Class __________ Date _______________