HOLYCROFT
Primary School and Nursery

E-SAFETY POLICY

2019-2020

Overview

Our eSafety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors. This eSafety Policy relates to other policies including behaviour, Child Protection, anti-bullying, personal, social and health education and citizenship.

This E-Safety policy was created by:

- Hannah Hurd (Assistant Head/Designated Safeguarding Lead)

The following people were consulted during the creation of this policy:

- G Morrison (Headteacher)
- The Governing Body

The Policy was completed in September 2019

The Policy was approved by the Governors in

The Policy is due for review no later than

This Policy incorporates the statutory guidance from 'Keeping Children Safe in Education' September 2016.

Policy Statement

The aim of this policy is to protect staff and pupils from risks involved in using ICT in activities relating to their learning or work. The safety of children at Holycroft Primary School is the primary concern and **all** adults working in school should consider their own use of ICT, e.g. Web technologies such as social networking sites, email, mobile phones etc. and ensure that they will not be compromised by any material that their pupils may encounter.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve Literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

The breadth of issues can be categorised into three areas of risk:

- content; being exposed to illegal, inappropriate or harmful material
- contact; being subjected to harmful online interaction with other users
- conduct; personal online behaviour that increases the livelihood of, or causes, harm

Some of the dangers of new technologies may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Access to unsuitable video/Internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- The risk of being subject to radicalisation by those with whom they make contact on the Internet.

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.

Roles in School

The Governing Body

Sanjida Sultana is a member of the Governing Body and has been appointed the role of Safeguarding Governor (including E-safeguarding).

Holycroft school has an Safeguarding Team which includes the following members:

Mr G Morrison (Head Teacher)

Mrs L Morgan (Deputy Head Teacher & Deputy Safeguarding Lead)

Mrs H Hurd (Assistant Head & Designated Safeguarding Lead)

Mrs B Beattie (SEND Lead and Deputy Safeguarding Lead)

Mrs K Fox (Family Liaison Worker& Deputy Safeguarding Lead)

Mrs P Walsh (Business manager)

Mrs J Vause (Attendance Officer)

Our school ICT technicians are Amar & Gareth from UDB Solutions . The Safeguarding Team will consult them regarding any technical issues related to the safeguarding and security of data.

The Safeguarding Team will meet Half termly to discuss and review policies and any E-Safety incidents.

The school will monitor the impact of the policy using:
● Logs of reported E-Safety incidents
● Smoothwall monitoring of network activity
● Pupil E-Safeguarding survey data which is gathered through annual Questionnaires.
● Evaluation of children's work
● Discussions at children's groups i.e. school council
● Monitoring planning and evidence of work
● Parental E-Safeguarding data which is gathered annually and through parent feedback.

Data from the questionnaires will be monitored annually and is used to develop staff training, parent meetings, planning and teaching.

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Responsibilities of the School Community

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other eSafeguarding incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate eSafeguarding behaviour that take place in or out of school.

The responsibilities outlined below show how each member of the school community contributes to eSafety:

	Responsibilities
Designated Safeguarding Lead (H. Hurd)	• Promote an awareness and commitment to eSafety throughout school. • Responding to notification of unsuitable use of ICT in school or incidence of unsuitable internet material by passing school filtering system. • Logging above incidences in eSafety incident log through 'Forensic Monitoring' system. • To attend latest eSafety training and implement in school at the next available opportunity. • Ensure that eSafety is promoted to parents and carers. • Devising, presenting and annually updating the schools eSafety policy for agreement by staff and governors. • Liaising with staff to ensure eSafety policy is adhered to by adults and children in school. • Be the first point of contact in school on all eSafety matters. • Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur. • Dealing with more serious breaches of policy and contacting appropriate bodies. • Take responsibility for the eSafety of the school community. • To hold a whole school assembly every half term to promote eSafety. • Should ensure staff undergo regularly updated Safeguarding training • Ensure thje curriculum for Esafety is robust including regular lessons in E safety, visits from E-safet policeman Luke Carson.
Governing Body	• Reading and agreeing eSafety policy annually to ensure safety of Pupils and staff at Holycroft Primary School in line with the school's Safeguarding Policy and 'Keeping Children Safe in Education Statutory Guidance for Schools and Colleges'. • Develop an overview of the benefits and the risks involved in using the Internet and other technologies used in school. • Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technologies in and out of school. • Ensure the school has appropriate filters and monitoring in place. • Should ensure staff undergo regularly updated Safeguarding training. • Ensure children are taught about online safety.

Technical Staff (Amar/Gareth –UDB Solutions)	• Read, understand, and promote the school's eSafety policy. • Report any eSafety issues to the Designated Safeguarding Lead. • Read, sign and follow the staff ACCEPTABLE USE AGREEMENT. • Be aware of current eSafety issues. • Maintain a professional level of conduct in their personal use of technology at all times. • Ensure the school's ICT infrastructures are secure and not open to misuse or malicious attack. • To make sure antivirus software is always up to date. • That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; eSafeguarding Officer for investigation / action / sanction • that monitoring software / systems are implemented and updated as agreed in school policies
Teachers & Support Staff (refer to 'Code of Conduct' for Employees)	• Teaching children about the correct use of ICT and ensuring they follow rules and procedures in the eSafety policy. • Supervise children carefully when engaged in learning activities involving technology. • Be aware of what to do should an eSafety incident arise. • Their responsible use of ICT in school and of devices provided by school for their use outside school, including effective anti-virus protection when accessing the internet at home. • Maintain a professional level of conduct in their personal use of technology at all times. • Read, sign and follow the staff ACCEPTABLE USE AGREEMENT. • Ensure hey have an up to date awareness of eSafeguarding matters and of the current school eSafeguarding policy and) • they report any suspected misuse or problem to the Headteacher / Safeguarding Lead • All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems • ESafeguarding issues are embedded in all aspects of the curriculum and other activities • In lessons where internet use is pre-planned pupils 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
Children	• Their correct use of ICT in school according to the eSafety policy. • Notifying their teacher if they encounter any incorrect use of

	ICT in school/home or unsuitable internet material. • Sign and follow the pupil ACCEPTABLE USE AGREEMENT. • Take responsibility for learning about the benefits and risk of using the internet and other technologies in school and at home. • Take responsibility for their own and each others' safe and responsible use of technology in school and at home. • Discuss eSafety issues with family and friends in an open and honest way. • To be aware of the appropriate age for Social Media and accessing various computer/video games.
Parents and Carers	• Help and support the school in promoting eSafety. • Read, sign and follow the ACCEPTABLE USE AGREEMENT. • Take responsibility for learning about the benefits and risks of using the Internet and other technologies that children use in school and at home. • Take responsibility for own awareness and learning in relation to the risks posed by new and emerging technologies. • Discuss eSafety with own children, encouraging them to behave safely and responsibly when using technology. • Consult the school if there any concerns about child's use of technology • Parents and carers will be encouraged to support the school in promoting good eSafeguarding practice and to follow guidelines on the appropriate use of: • Digital and video images taken at school events • access to parents' sections of the website and on-line student / pupil records • Attend eSafety presentations organised by school. • To be aware of the appropriate age for Social Media and the accessing of various computer/video games.

Teaching and learning

Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Staff will refer to the Scheme of Work (E-safety objectives) written by The Bradford Authority team.

Pupils will be taught eSafety lessons.

E-Safety and digital literacy and ctizenship will be included in a clear and progressive curriculum, to ensure that pupils know how to conduct themselves online in a safe and appropriate manner.

- School will provide a series of specific eSafety-related lessons in every year group; this will be carried out through the PSHCE curriculum and as part of the Computing curriculum – an E-Safety lesson will be taught once a half term.
- eSafety will be promoted through an assembly every half term and whole school activities, including the promotion of eSafety Day and Safer Internet Day.
- E –Safety lessons taught by – Luke Carson (Police Officer – Internet Safety)

Parents and Carers eSafety Involvement

The school will take every opportunity to help carers and parents to understand issues related to ESafety. We will assist parents to understand key issues in the following ways;

- *An annual parents' E-Safety information session, with a presentation; regular newsletters, offering parents advise on the use of the internet, gaming and social media sites at home.*

- *Policies/E-Safeguarding September 2019*

- *Ensuring their child understand the issues surrounding E-Safeguarding*

- *Endorsing the Pupil Acceptable User Policy. Please note pupils will not be given access to the school network until the Acceptable Use Policy has been signed by both pupil and parent/carer and returned to the school officeIt is of the upmost importance to help to develop parental knowledge, skills and understanding of eSafety.*

Managing ICT Systems and Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by ICT technicians (ICT suite and teacher laptops).
- Security strategies will be discussed with the BLN.
- E-safe software installed and monitored on all school PCs, staff laptops and child net books.
- Pupils will log on using an individual username and will be supervised carefully when using the Internet.
- Staff will log on using an individual username, which they will keep secure. Staff will ensure they log out after each session and not allow pupils to access the Internet through their username.
- Any administrator passwords for the school ICT system will be kept secure and will be available to the Head teacher, Computing Coordinator and technical support.

Managing filtering

- The school will work with the BLN and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved, ensuring that access to illegal and inappropriate online content is blocked.
- ICT technicians will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all the users.

Monitoring Strategies

- If staff or pupils discover an unsuitable site, it must be reported to the Designated Safeguarding Lead and appropriate action will then be taken.

- E-safe software will monitor filtering and provide weekly reports to be reviewed by the Headteacher/Designated Safeguarding Lead and appropriate action taken.

Learning Technologies in School

Pupils know the school maxim of 'Click and Tell'
This underpins their responses.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils will be reminded about sending polite, responsible e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils will be warned about the dangers of opening e-mails from an unknown sender and opening attachments.
- E-mails sent to an external organisation should be written carefully.
- The forwarding of chain letters is not permitted for both staff and pupils.
- All staff will be allocated a secure school email address.

Published content and the School Website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- All school policies(including the eSafety Policy) will be available on the School Website.

Publishing images, videos and sound

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained when pupils join the school allowing photographs/videos of pupils to be published on the School Website.
- Digital images, video and sound will only be created using school equipment.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- In school staff are only allowed to access social networking sites relating to the schools twitter account using school equipment e.g. laptops, iPods/iPads, suite pc's etc.

- Staff members are only allowed to access the school twitter account.
- Pupils will not access social networking or file sharing sites on school net books e.g. Facebook, MSN, snap chat, Instagram
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Using Mobile Phones and Smart Watches (refer to Staff Code of Conduct)

- Staff who are in contact with pupils should not use their mobile phones during their directed hours/paid hours of employment, unless they are a member of the Senior Leadership Team or have the permission of the Headteacher. Outside of directed hours, mobile phones should only be used where pupils are not present.
- Mobile phones/ watches are not to be used to take photographs or videos of the children at any time. Any photograph/video must be taken on school equipment.
- Pupils are not permitted to bring mobile phones or Smart Watches to school unless authorised by the Headteacher (must be handed in at the school office and kept secure during school hours).
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will not be expected to use their mobile phone in any situation where a parent or pupil may be able to observe personal details.
- **Staff are not permitted to use their own phone or camera to take photos during trips.**

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and introduced into school as appropriate.
- The eSafety Policy will be amended accordingly to reflect any new technology that may cause an eSafety risk.

Video conferencing (e.g. Skype, Face time)

School will use video conferencing to make links with other communities. It will be done in a safe and responsible manner.

- All video conferencing will be carried out and supervised by an adult.
- Parental permission will be sought before taking part in video conferencing.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR regualtions.
- Staff will make sure they log off from a computer after accessing personal data.

- Staff will not remove personal data from the school premises without ensuring the data is secure i.e. use encrypted memory sticks. This is with the exception of the following:
  1. Emergency contact details on school trips, which should be destroyed as confidential waste after the trip has taken place.
  2. If it is a specific requirement of the staff member's role and has been agreed by the Headteacher
  3. When attending meetings off the school premises, where it is a requirement and has been agreed by the Headteacher
- All personal data MUST be returned to school at the earliest opportunity.

The School Website and other online content

- All content will be approved by the Headteacher/Safeguarding Lead before publication.
- The School Website will contain no personal details of any staff or pupils.
- Staff and pupils should not post school related content on any external website without consent from the head first.
- Only designated staff are allowed to tweet on the schools Twitter account.

Twitter Account

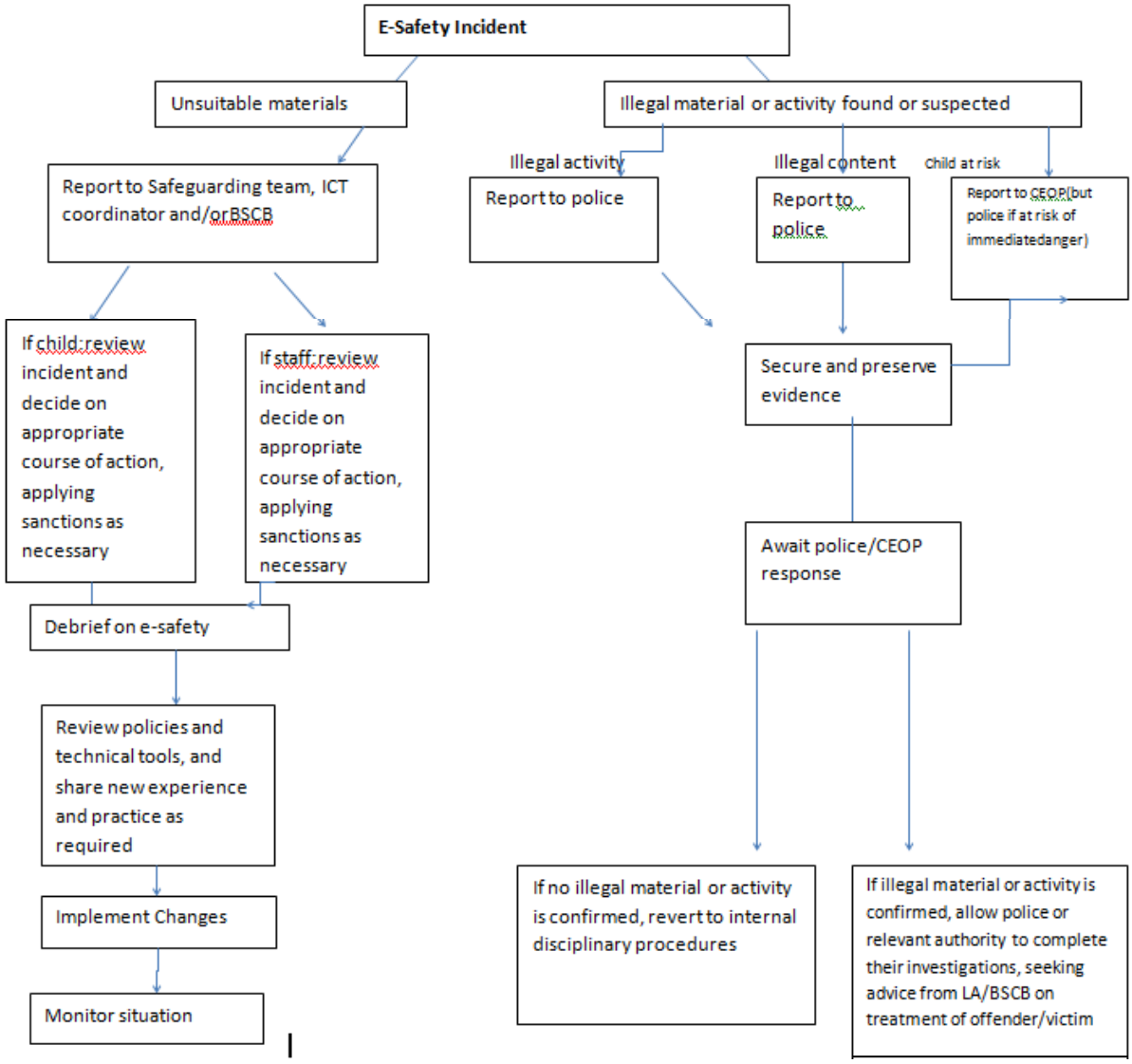
The school has an official Twitter page, managed by Mr Geoff Morrison.

Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Dealing with eSafety incidents

Reporting e-safety incidents flowchart



(reproduced from 'ACCEPTABLE USE AGREEMENTs in Context: Establishing Safe and Responsible Online Behaviours', Copyright Becta 2009)

Policy Decisions

Authorising Internet access

- All staff or adults using school ICT equipment must read and sign the 'Acceptable ICT Use Agreement'.
- The school will keep a record of all staff and pupils who are granted Internet access.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the BLN can accept liability for the material accessed, or any consequences of Internet access.
- The school will annually audit ICT provision to establish if the eSafety policy is adequate and that its implementation is effective.

Handling eSafety complaints

- Complaints of Internet misuse will be dealt with by the school Safeguarding lead or Head Teacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the appropriate body i.e. police, social services, CEOP, LEA to establish procedures for handling potentially illegal issues

Preventing Radicalisation

The Prevent Duty Since 2015, when the Government published the Prevent Strategy, there has been an awareness of the specific needs to safeguard children, young people and families from violent extremism. There have been several occasions nationally in which extremist groups have attempted to radicalise vulnerable people to hold extreme views including views justifying political, religious, sexist or racist violence, or to steer them into a rigid and narrow ideology that is intolerant of diversity and leaves them vulnerable to future radicalization. Holycroft Primary School is clear that this exploitation and radicalisation should be viewed as a safeguarding concern.

The school reduces the risk of radicalisation through its strong ethos, the promotion/celebration of British Values, the taught PSHE curriculum and activities that promote community cohesion. E-Safety teaching and learning also ensures that children know how to report any concerns and have strategies and knowledge to keep themselves safe online

The use of films in education

All films watched by children in school will have a 'U' certification. If films are classed as a 'PG' this will be at the discretion of the teacher. On admittance to the school, parents will be asked to sign a consent form to say that they agree to their child watching films rated 'PG' if considered appropriate by the class teacher.

The Internet

To a large extent we rely upon the internet filtering facility provided by our Internet Service Provider ***BLN*** and E-safe software to protect Holycroft Primary School users from inappropriate internet material. However, this is not infallible, hence the need for the following strategies and procedures to be part of our policy in the event of material getting through the filter.

When using the internet with interactive whiteboards Teachers should, as much as possible, use websites they have previously visited, having saved the addresses and accessing the sites through hyperlinks.

If "surfing" the internet in lessons projectors should be set to **freeze**, **mute or switched off** until appropriate content has been found.

When children's learning involves their use of internet sites it is advisable that they should be directed to sites specified by teachers and accessed through hyperlinks on prepared and stored documents on the schools network.

Children's use of search engine facilities in school should take place only when

- They have been taught about internet safety. This will begin in Year 1 and be revisited at least termly.
- They know what to do should they encounter inappropriate material (C.A.T. – Click and Tell).

In the event that inappropriate internet material is encountered the following steps should be taken by children and teachers

1. Do not leave the website until its address has been recorded. This will enable the ISP to be notified and relevant action taken to prevent future access.
2. Turn off the monitor or minimise the page if working on a laptop.
3. Pupils should tell their teacher immediately.
4. Teachers should note the address of the site or, if NGFL is in the address box right click and save it to favourites to be accessed later.
5. The schools Designated Safeguarding Lead should be notified as soon as possible.
6. The Designated Safeguarding Lead will "blacklist" the site and ring the relevant department of the Internet Service Provider to notify them.
7. The Designated Safeguarding Lead will log action taken.

Email, Social networking and Mobile Phones

In school **pupils** will be allowed to send and receive emails only in lessons. They will have been taught about the relative areas in eSafety (e.g. non-disclosure of personal information, dealing with cyber bullying) before such lessons take place. They will know that the content of their emails can be monitored by the school's eSafe software for unsuitable content, and they will know the consequences of sending such content.

In the event of receiving unsuitable emails/text messages/chat room dialogue etc. the following procedure should be followed

- Do not delete the email until it has been dealt with (print it if possible)
- Notify your teacher immediately if the email is received at school or your parents if it is received at home
- The school's Designated Safeguarding Lead to take action to establish the source of the email and arrange for relevant sanctions or further action
- The Designated Safeguarding Lead will record action taken

In the event that "cyber-bullying" which takes place outside school has repercussions in school, action will be taken in line with the school's anti-bullying policy.

It is the responsibility of teachers to ensure appropriate supervision in lessons and to ensure that children have learned about the relevant areas in eSafety *before* using email in school. Social Networking sites should not be accessed in school. **Staff** should acquaint themselves with the relevant statements in the Acceptable Use section of this policy.

Sexting

Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of a child sent by the child. If an incident involving child produced sexual imagery comes to the school's attention it should be reported to the DSL in school. The school should then follow the schools Child Protection Policy and report to the police. School will follow guidance from 'Sexting in Schools and Colleges'.

Pupil Sanctions for misuse of ICT

Staff will follow the behaviour policy and the Child Protection policy.

Introducing the eSafety Policy to pupils

- eSafety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and i every E –Safety lesson.
- Pupils will be informed that network and Internet use will be monitored.
- eSafety rules will be posted on log in screen of school PC's.

Staff and the e-Safety Policy(refer to Staff Code of Conduct)

- All staff will be given the School eSafety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff must exercise caution when using Information Technology and be aware of the risks to themselves and others. Staff must not use Social Media (e.g. Facebook) with pupils or former pupils.
- Staff must not engage in inappropriate use of Social Network sites which will bring themselves, the school, the school community or employer into disrepute.
- When concerns with parents and pupils arise, staff must only use the school email account for professional reasons and not use personal accounts.

Enlisting parents' support

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school Website.
- ACCEPTABLE USE AGREEMENTs will be agreed and signed by all children and parents/carers.

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 the Headteacher.

Appendices:

1. **Acceptable Use Agreement – pupil**
2. **Acceptable Use Agreement – staff**

Pupil Acceptable Use Agreement / eSafety Rules

Dear Parent/ Carer

ICT including the internet, email, laptops, digital cameras etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT at school.

Please discuss these e-Safety rules with your child. If you have any concerns please refer to the school website (http://www.holycroftprimary.org.uk/) where there are links to other helpful sites with a wealth of information on this subject.

 I will only use ICT in school for school purposes.
 I will only use my class email address.
 I will make sure that all ICT contacts with other children and adults are responsible.
 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 turn off my monitor and tell my teacher immediately.
 I will not send to children or adults anything that could be considered unpleasant or nasty.
 I will not give out my own details such as my name, phone number or home address.
 I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
 I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
 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 eSafety.

Child signature

We have discussed this and _____ agrees to follow the eSafety rules and to support the safe use of ICT at Holycroft Primary School.

Signature _____ Date _____

Staff Acceptable Use Agreement / Code of conduct

ICT and the related technologies such as email, the Internet and mobile phones 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 school e-Safety coordinator.

 I will only use the school's email / Internet 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(s) for any school business.

 I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I will use an encrypted memory stick if I need to transfer data.

 I will not browse, download or upload material that could be considered illegal or dangerous to minors.

 I will not send to pupils or colleagues material that could be considered offensive or illegal.

 Images of pupils will only be taken on school equipment and will only be used for professional purposes. They will not be distributed outside the school network without the permission of the parent/ carer.

 I will only use my mobile phone outside of directed time, unless permission has been given by the Headteacher.

 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 Headteacher.

 I will respect copyright and intellectual property rights.

 I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature …… Date ……

Full Name ……