Hothfield Junior School
E-Safety Policy
September 2014

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, 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.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- 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
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The E-safeguarding Committee

James Procter – E-safeguarding Leader (Headteacher, Child Protection named person)
Isobel Fairburn – Computing Subject Leader
Ian Crosby – Safeguarding Governor
Corrine McKittrick -School IT Technician
The committee will consult HiTech- our technical support - over technical issues related to safeguarding and security of data.

Development and Review of this policy.

This e-safeguarding policy was approved by the *Governors Personnel committee*	
The implementation of this e-safety policy will be monitored by the:	*The E-safeguarding committee*
Monitoring will take place at regular intervals:	*Twice yearly*
The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of	September 2015

any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Children's services (Keighley) Jenny Sadowski Safeguarding Officer Bradford Council Bradford Learning Network

Monitoring the impact of the policy

The school will monitor the impact of the policy informed by:

- Logs of reported incidents in the e-safeguarding incident log – a supplement to the Headteacher's Serious Incident Log
- Internal monitoring of network activity
- Smoothwall user logs. Our technician can access these logs to see which users accessed which web sites at which times.
- Student e-safeguarding data will be gathered through the use of the Bradford Council Children's Services eSafeguarding questionnaire available at: http://bradfordschools.net/limesurvey/ . Progress will be monitored at the start of each academic year. The next completion of the survey will be in early Autumn 2014. – Report to E-Safety Committee
- E-safe monitoring system – weekly monitoring reports to the headteacher of computing activity in school through our subscription to E-Safe Systems Ltd

Roles and Responsibilities

Govemors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Personnel Committee receiving regular information about e-safety incidents and monitoring reports

The Governor responsible for child protection Ian Crosby has taken on the responsibility for e-safeguarding.

The role of this governor will include:

- regular meetings will include-safeguarding where e-safeguarding issues will be discussed
- regular monitoring of e-safety incident logs – reported to Personnel Committee
- reporting to relevant Governors through minutes of the Personnel Committee.

Headteacher and Senior Leaders:

- The Headteacher is the designated E-Safety Coordinator responsible for ensuring the-safeguarding (including e-safety) of members of the school community
- The Headteacher/ E-safeguarding leader is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Safeguarding Policy and the Managing Investigations Procedures adopted by the school..

E-Safeguarding Leader

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends the Governors Personnel Committee (which discusses e-safeguarding issues).

Network Manager / Technical staff:

The school technician ensures:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that s/he keeps up to date with e-safety technical information and updates the E-safeguarding leader or ICT coordinator as relevant.
- that monitoring software and anti virus software is implemented and updated

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
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety leader for investigation
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities . E-safeguarding lessons are taught as necessary across the school year and in particular during the annual e-safety week.

- they continually promote the SMART code for online safety (See Appendix 1)

- students / pupils understand and follow the school e-safety and acceptable use policy
- 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

Named person for child protection

James Procter, Su Cloke and Jennie Hudson are the Designated Senior People for Child Protection.

They are trained in e-safety issues and are 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

Children

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign in September before being given access to school systems.

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e-safeguarding. We will assist parents to understand key issues in the following ways:

Regular parents e-safeguarding evening/ daytime presentations.

Regular newsletters offer parents advice on the use of the internet and social media at home.

The SMART Code (see appendix 1) is shared with parents each year during the E Safety Week and parents are encouraged to enforce the code at home.

Education – Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A planned e-safety programme is delivered through the year and in particular during the annual E-Safety Week.
- The Bradford ICT Scheme of work also highlights e-safeguarding issues that arise in the context of ICT lessons.
- Key e-safety messages are reinforced as part of the annual e-safety assembly.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the research strand of the Bradford ICT scheme of work.
- Students will sign the Acceptable Use Policy and it will be on display in the Computing Room.

- Pupils 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. Evaluation and cross referencing of sources is covered in the research strand of the Bradford ICT scheme of work which the school follows.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Multimedia and Sound strands of theBradford ICT scheme of work which the school follows.

Education - Staff Training

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 Staff meeting covering e-safeguarding will take place regularly – at least annually linked to the E Safety Week. This may be delivered by a member of Bradford Council Children's Services Curriculum ICT Team or a member of the E-safeguarding Committee.**
- **All new staff should receive e-safety training as part of their child protection induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.**

Education - Governor Training

Governors take part in e-safety training / awareness sessions – either parent or staff.

Cyber-Bullying

The sending of unkind, unfriendly or hurtful texts or messages to another child is wrong and constitutes cyber-bullying. The Pupil Acceptable Use Agreement (Appendix 3) makes it clear to children that this is not acceptable. If children receive such messages out of school they are encouraged to report it to an adult in school so the school can investigate and respond.

Internet Provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity.

The school subscribes to the e-safe monitoring system through E-Safe Systems Ltd and the J2E system. These systems monitor all computing usage in school and provide the e-safety leader with weekly monitoring reports highlighting any inappropriate usage.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils 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 online.
- Staff are allowed to take digital / video images to support educational aims. Staff may use their own equipment to take a photograph of a child to upload to the school website/ for school use – for instance, a smartphone to upload a photograph to the blog. All images of school pupils must be immediately deleted from the member of staff's equipment once uploaded to the school site/ for school use. This should be done as soon as possible.

- Photographs of children published on the website or blog must not contain full names.
- Parents or carers are given the opportunity to deny permission for photographs of students / pupils to be published on school publications (see form in appendix)

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices such as memory sticks.

Appendix 1:

We promote the SMART rules from www.kidsmart.org.uk and www.childnet.com

Safe: *Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.*

Meeting: *Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.*

Accepting: *Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!*

Reliable: *Information you find on the internet may not be true, or someone online may be lying about who they are.*

Tell: *Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.*

Appendix 2: Hothfield Junior School
ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Agreement. Members of staff should consult the school's e-Safety Policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that my use of school information systems (e.g. SIMS), Internet (including email) and any other networked ICT resources will be monitored and recorded to ensure Policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than on request from an authorised member of staff (including but not limited to the named persons for e-Safety, ICT Co-Ordinator, Business Manager and external technical support provider).
- I will not install any software (including mobile apps) or hardware without permission from the ICT Co-Ordinator.
- I will ensure that pupil data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. Any hardware on which pupil data is stored will be password protected.
- I will adhere to copyright and intellectual property laws and only publish media which I own, have permission to use or is copyright-free.
- I will report any incidents of concern regarding children's safety whilst using new technologies in or out of school to the e-Safety Officer.
- I will ensure that electronic communications with pupils including blog comments and email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I understand that befriending pupils on instant messaging services and social networking sites is prohibited.
- I may use my own equipment to take a photograph of children to upload to the school website/ for school use – for instance, a smartphone to upload a photograph to the blog. All images of school pupils must then be immediately deleted from my equipment once uploaded to the school site/ for school use. This should be done as soon as possible.
- I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the ICT Acceptable Use Agreement for Staff.

Name: …… Signed: …… Date: ……

Appendix 3: Pupil Acceptable of ICT in School Agreement

- We only access the computer system with the login and password we have been given
- We don't access other people's files or use their password and login details
- We ask permission before using the Internet
- We immediately hide any webpage we don't like and inform a teacher
- We only email people our teacher has approved
- We send emails that are polite and friendly
- We never use the internet, email or texts to send unfriendly, unkind or hurtful messages. This is cyberbullying.
- We will immediately report any unpleasant messages received as this would help protect other children and ourselves
- We never give out a home address, phone number, passwords or other personal information.
- We never arrange to meet anyone we have met over the Internet
- We never open emails sent by people we don't know
- We tell the teacher if we see anything on a device we are unhappy with
- We will not alter the settings on any device without the permission of the teacher
- We will not download any software or programs on to a device without the permission of the teacher

- We understand that we are responsible for good behaviour on the Internet and when using ICT equipment, inappropriate use may lead to access being withdrawn

Signed: Date:

.

Appendix 4 Photograph / video consent form

Dear Parents/Carers

At Hothfield Junior School we take the issue of child safety very seriously, and this includes the use of images of pupils.

Including images of pupils in publications and on the school blog or website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact. We will never include the full name of the pupil alongside an image. Any use of pupil images at Hothfield Junior School is underpinned by our Internet Safety Policy.

We ask that parents consent to the school taking and using photographs and images of their children. **IF YOU DO NOT CONSENT TO THE SCHOOL TAKING AND USING PHOTOGRAPHS AND IMAGES PLEASE COMPLETE THE SLIP BELOW.**

If we do not receive any notification, we will assume that you consent to the school taking photographs for use in publications and on the school website.

Kind regards

Mr James Procter

Headteacher

✂……

I DO NOT wish photographs and digital images of the child named below appearing in any publications or on the school website.

Name of child ……. Class ……..

Signed …… Date ……..

Name of Parent/Carer ……..