HEATH FIELDS PRIMARY SCHOOL

ONLINE SAFETY POLICY

1. Introduction and overview

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

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

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

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

At Heath Fields Primary School we understand the responsibility to educate our pupils in online issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet technologies provided by the school; (such as PCs, laptops, netbooks, iPad's, whiteboards, digital video equipment, etc); and also technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc). However, it is important to stress that pupils can only bring in mobile devices in exceptional circumstances with prior consent from teaching staff.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Heath Fields Primary School with respect to the use of computing technologies.
- safeguard and protect the children and staff of Heath Fields Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

2. Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinator in our school is **Mrs F Paterson** who has been designated this role as computing coordinator. She will be working alongside the designated safeguarding leads in this role where appropriate. All members of the school community have been made aware of who holds this post. It is the role of both the head teacher and the online coordinator to keep abreast of current issues and guidance through organisations such Derbyshire LEA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head-teacher and online coordinator updates other members of Senior Management and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice where necessary.

The roles of different members of our school community can be summarised as follows:

Role	***Key Responsibilities***
Headteacher / Designated Child Protection Lead	• To take overall responsibility for online safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable safeguarding training to include online safety • Alongside the online safety coordinator, to keep abreast of any matters regarding online safety • To take the lead in the event of a serious online safety incident. • To liaise with the computing technician to ensure filtering and monitoring meets current guidelines. • To ensure that an online safety incident log is kept up to date • Liaises with the Local Authority and relevant agencies if necessary

	• Takes day-to-day responsibility for online safety issues
Online Safety Co-ordinator / Computing Lead Teacher	• Has a leading role in establishing and reviewing the school online safety policies / documents • Promotes an awareness and commitment to online safeguarding throughout the school community • Ensures that online safety education is embedded across the curriculum • Ensures that a progressive scheme of online safety education is being followed across the school and taught discretely where necessary • Oversees the delivery of the digital literacy element of the Computing curriculum • Alongside the designated safeguarding lead, to keep abreast of any matters regarding online safety and disseminating this information to staff • Liaises with the computing technician where appropriate • To be aware of procedures to be followed in the event of a serious online safety incident and provide a supporting role to the head teacher. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • Facilitates training and advice for all staff • Is regularly updated in online safety issues and legislation
Governors	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. • A member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing technician	• To keep virus protection up to date • To ensure the security of the school computing system • The school's web filtering is monitored and updated on a regular basis • They keep up-to-date with the school's online safety policy and technical information in order to effectively carry out their role and to inform and update others as relevant • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures

Teachers

- To embed online safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff

- To read, understand and help promote the school's online safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement
- To be aware of online 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
- To report any suspected misuse or problem to the Head Teacher
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Writing and reviewing the online safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

The online safety policy and its implementation will be reviewed annually by the online safety coordinator.

Online safety skills development for staff

- Our staff receive regular information and training on online safety issues through the coordinator at staff meetings and as part of safeguarding training (at least annually).
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate online safety activities and awareness within their lessons, both cross-curricularly where appropriate and also in discrete online safety teaching.

Online safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website and/or on social media.
- An online safety letter is sent out annually to parents to coincide with the national online safety day.
- The school will also send out relevant online safety information through newsletters, the school website and the school prospectus as deemed necessary.

Community use of the Internet

- External organisations using the school's computing facilities must adhere to the online safety policy and the acceptable use policy for adults where appropriate.

3. Expected Conduct and Incident Management

Expected conduct

At Heath Fields Primary School, ***all users***:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand 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 and using images and on cyber-bullying

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- should have a good understanding of research skills and acting responsibly and safely online.

Incident Management

At Heath Fields:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- support is actively sought from other agencies as needed
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- parents / carers are specifically informed of any online safety incidents involving young people for whom they are responsible.

4. Teaching and Learning

Internet use will enhance learning

Our school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Educates pupils on the dangers of technologies that may be encountered outside school- this can be done informally when opportunities arise and as part of the online safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- If anything that causes alarm or distress does appear while pupils are accessing the internet, all pupils will be aware of the procedures to follow; to either minimise the internet browser or turn off the monitor and make the teacher aware as soon as possible.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

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.

5. Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly by the computing technician.
- Virus protection will be updated regularly.
- Security strategies will be discussed between the computing technician, the computing coordinator and the head teacher.

E-mail

If and when e-mails are utilised by pupils, the following must be adhered to;

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

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 (with the exception of the names of staff). The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully to ensure only pupils with consent appear on our website or school social media accounts.
- *We follow the following rules for any external use of digital images:*
    - If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.
    - Where showcasing examples of pupils work we only use their first names, rather than their full names.
    - If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parents/carers for personal use

On the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites or on social media, e.g. School performances and assemblies etc.

Social networking and personal publishing

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school and they will be dealt with as according to our anti-bullying policy.
- School staff are advised not to add pupils as 'friends' if they use these sites.

- It is advised that staff do not add past pupils as 'friends' while they are under the age of 25. Although in the cases where past pupils are also family friends, it is acknowledged that this situation may occur, but as long as this prior advice has been carefully considered.

Managing filtering

- The school will work alongside our computing technician to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, Online Safety Coordinator or Head teacher immediately.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing mobile technologies

- The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be kept by the class teacher and they will be kept in a secure environment until the end of the day.
- The sending of abusive or inappropriate text messages outside school is forbidden. Any cases of this will be investigated thoroughly by senior members of staff if brought to their attention.
- Staff will use a school phone where contact with parents is required unless there is exceptional circumstances (such as on a school trip).
- Staff should not use personal mobile phones during designated teaching sessions or when directly supervising children (unless in exceptional circumstances such as a school trip).
- Mobile phones should not be kept in classrooms and may only be used in areas away from pupils, such as the offices or in the staff room.
- Mobile phones brought into school are entirely at the staff member or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

6.Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Heath Fields Primary School
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school and Derbyshire LEA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school. For other members of the community, the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Derbyshire LEA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school (whichever is the longer period of the time out of the two circumstances). We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Derbyshire County Council and as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

7. Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must abide by the school's online safety rules and the pupil's Acceptable Use Policy.
- Parents will be asked to sign the Acceptable Use Agreement for Key Stage 1 pupils giving consent for their child to use the Internet in school by following the school's online safety rules and within the constraints detailed in the school's online safety policy. Pupils at Key Stage 2 will be expected to sign the Key Stage 2 Acceptable Use Agreement.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school computing resource.

Password Security

- Adult users are provided with an individual network and email login username and password, which they are encouraged to change periodically.
- All year groups are provided with an individual network password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

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 DCC can accept liability for the material accessed, or any consequences of Internet access. The school will audit computing provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the online safety coordinator/head teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety coordinator/designated safeguarding lead/ head teacher and recorded.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with by the designated safeguarding lead in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

8. Communications Policy

Introducing the online safety policy to pupils

- Online safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year, as well as the annual online safety day which we observe each year in February.
- Teaching staff will deliver a progressive scheme of online safety work by following the school's online safety curriculum. Evidence of this work will be collated by the computing coordinator. This will be taught discretely.
- Pupils will be informed that network and Internet use will be monitored**.**
- Children will be informed of the procedures in place for dealing with inappropriate websites as mentioned previously in this document.

Staff and the online safety policy

- All staff will be given the School Online Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

9. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Online Safety Coordinator.

Ongoing incidents will be reported to and monitored by the head teacher, the designated safeguarding leads and the Online Safety Coordinator.

The Online Safety Policy will be revised by the Online Safety Coordinator.

Date implemented: December 2016
Date for review: December 2017

Signed: …… (Headteacher)

Approved by the Governing Body of Heath Fields Primary School.

Signed: …… (Chair of Governors)

Date: