Working together to inspire every pupil to:
Step in to their learning adventure.
Step up to achieve their potential.
Step out and let their creativity shine.
Step together in friendship and respect.
Step forward and follow their dreams.

Address: Parkway, Chellaston, Derby DE73 5NY
Tel: 01332 691351
Web: www.homefields.derby.sch.uk
Email: admin@homefields.derby.sch.uk
Headteacher: Mrs S E Coleman

Online Safety Policy

Name of school: Homefields Primary School

Date of policy publication: March 2020

Author/s of policy: Homefields Primary School

Date of last review: March 2019 **Date of next review:** February 2021

Policy review dates and changes

Review date	By whom	Summary of changes made	Approved by
March 2020	M. Draper		Name: S.Coleman

Computing Coordinator – Milly Draper

Introduction

The School's Online Safety Policy is to raise awareness of the safety issues associated with information systems and electronic communications. "Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks" (DfE, 2019)

Online Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones, tablets and other wireless technology. The Policy highlights the need to educate staff, children and young people about the benefits, risks and responsibilities of using information technology. It raises awareness and provides safeguards to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mails, blogs and social networking all transmit information using the Internet's communication infrastructure. Anyone can send messages, discuss ideas and publish material with little restriction, thus making it an invaluable resource used by millions of people every day. However, much of the material published online is for an adult audience and some is unsuitable for children. Pupils must learn that publishing personal information could compromise their security and that of others.

It must be made clear to pupils, staff and visitors that inappropriate use of school technologies is unauthorised and will result in serious consequences. Schools should be aware that a disclaimer is not sufficient to protect a school from a claim and the school needs to ensure that all reasonable actions have been taken and measures are put in place to protect users.

Legislation

The following legislation must be considered when following this policy:

- Human Rights Act 1998
- Data Protection Act 1998

The new government guidance 'Teaching online safety in school (DfE, June 2019)' is also to be taken into consideration.

Scope of the Policy

The 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 the school ICT systems, both in and outside of 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 school site and empowers members of staff to respond to incidents of inappropriate behaviour. This is pertinent to incidents of cyber-bulling, sexting, grooming or other online safety incidents covered by this policy, which may take place outside of school, but is linked to membership of the school and/ or safety of pupils.

The school will deal with such incidents within this policy and will inform parents/ carers of incidents of inappropriate online safety behaviour that takes place either in or out of school.

Teaching and Learning

Pupils:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's computing provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities provided in the following ways:

- A planned Online Safety curriculum should be provided as part of Computing/ PSHE and should be regularly revisited throughout the year.
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/ content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using materials accessed from the internet.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt a safe and responsible use of ICT, both within and outside of school.
- Staff should act as good role models in their use of digital technologies, the internet (including social networking) and mobile devices.
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use (e.g. using child friendly search engines) and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff **must** be vigilant in monitoring the content of the websites young people visit.

Authorising Internet Access:

In foundation stage and at Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved online material. Pupils will be taught about safe internet use and what to do if unpleasant internet content appears.

At Key Stage 2, pupils will be taught about safe internet use and how to report unpleasant internet content to the Online Safety coordinator in school and the CEOP Report Abuse icon whilst out of school.

Parents/ carers:
Some parents and carers have a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children, in the monitoring of their children's online behaviour and the protection of their safety. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- The school website has direct links to E-safety news and to the Child Exploitation and Online Protection Centre (CEOP) website, where advice on parental controls and restrictions can be found.

Staff/ Volunteers:
It is essential that all staff receive Online Safety training and understand their responsibilities.

- All members of staff and volunteers entering school must have read, understood and signed a copy of the school's Acceptable Use Policy.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings/ INSET days. Teachers must ensure support staff are fully aware of their role in the enforcement of Online Safety.
- All teachers receive monthly updates of current safeguarding news and issues.

Managing Internet Access

The school's ICT systems security, virus protection, filtering and monitoring will be reviewed regularly by Chellaston Academy Technicians. They will support the school in ensuring that the school network is a safe and secure as is reasonably possible.

- School technical systems will be managed in ways that ensure the school meets recommended technical requirements.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider. Requests for filtering changes must go through the Head teacher/ E-safety officer.
- If staff or pupils come across unsuitable online materials, the site must be reported to the Online Safety coordinator and Chellaston Academy technicians
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, mobile devices, etc.

Published content:

- Staff or pupil personal contact information, will not generally be published. The contact details given on the school website is for the school office. In special circumstances, staff may use their work email address to contact parents.
- The school will seek parental consent before publishing any pupil photographs or work.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
- Pupil's full names will not be used anywhere on the school website or any other online platform, particularly in association with photographs.

Social Networking and Personal Publishing

- The school will control and restrict access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised to never give out personal information of any kind that may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites and online gaming.

Video Conferencing and Webcam Use:

- Video conferencing should use the educational broadband network to ensure quality of service and security.
- Video conferencing and webcam use will be appropriately supervised for the pupil's age.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders:

- The Headteacher (Designated Safeguarding Lead) and Assistant Head Teachers (Deputy Safeguarding Leads) have a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher, Assistant heads and the Senior Leadership team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring the relevant staff receive suitable training to enable them to carry out their online safety roles and then train other colleagues, as relevant.

Network Manager/ Technical Staff (Chellaston Academy):

- Chellaston Academy Technicians will ensure that the school's technical infrastructure is secure and not open to misuse or malicious attack.
- Chellaston Academy Technicians will ensure that the school meets the required e-safety technical requirements.
- Chellaston Academy Technicians will ensure that the use of the network/ internet is regularly monitored in order that any misuse or attempt to misuse can be reported to the Headteacher for investigation and action.

Teaching and Support Staff:

- All staff must be responsible for ensuring that they have an up to date awareness of online safety matters and of the current school online safety Policy and practices.
- All staff must have read, understood and signed the school Acceptable Use Policy (AUP)
- All staff must report any suspected misuse or problem to the Designated safeguarding lead/ deputy for investigation and action.
- All digital communications with pupils and parents/ carers should be on a professional level and only carried out using official school systems.
- Teaching staff must ensure online safety issues are embedded in all relevant aspects of the curriculum and other activities, including PSHE.
- Staff must ensure that pupils understand and follow the online safety and Acceptable Use Policies.

Pupils:

All pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.

- Pupils need to know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Pupils will be expected to know and understand policies on the use of mobile devices and digital cameras within school. They should also know and understand policies on the taking/ use of images and on cyber-bullying.
- Children's personal mobile phones and devices are kept safe during school hours by their teacher, in order to safeguard children.
- Pupils should understand the importance of adopting good online safety practice when using digital technologies outside of school and realise that the school's online safety policy covers their actions outside of school, if related to their membership of the school.

Parents/ Carers:

Parents/ carers play a crucial role in ensuring that their children understand the need to use the internet and mobile device in an appropriate way. The school will take every opportunity to help and support parents understand these issues through parent's workshops and signposting important and relevant information through the school website. Parents/ carers will be encouraged to support the school in promoting good online safety practice and follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Their children's personal devices in school (where this is allowed).