Hall Orchard Barrow CE Primary School (Academy)

E-Safety Policy

Introduction

The rapid development of technology is having an increased impact on our everyday lives. At Hall Orchard, we enjoy extending our pupil's learning experience using technology. However, clear guidelines need to be established and adhered to, ensuring pupils, staff and parents are aware of the potential dangers of using technology, in particular electronic communication. Safe and courteous use of the internet, texting, email, and social media sites are areas that require specific education. This is known as e-Safety.

E-Safety highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. At Hall Orchard, we understand the responsibility to educate our pupils on e-safety issues, teaching them the appropriate behaviour, attitude and skills to enable them to remain both safe and legal when using the internet and related technologies. With this in mind, our Computing curriculum has focused e-Safety lessons and core e-Safety themes are embedded throughout the academic year. This is further enhanced by an annual e-Safety week (held every February to coincide with Safer Internet Day) across the school.

The school's e-Safety policy operates in conjunction with other policies including the Safeguarding policy and the Behaviour policy.

All staff and stakeholders must abide by acceptable use agreements.

Cyberbullying

Hall Orchard recognises there is a need to safeguard the welfare of all those within the school community and to encourage a culture of co-operation, acceptance and harmony both within and outside school. Hall Orchard believes that everyone in the school community has the right to learn and to teach in a supportive and caring environment without fear of being bullied. We are committed to helping all members of the school community to benefit from information and communication technology, whilst understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly. We have high expectations of all pupils, staff and parents and strive to create a school community in which all children can fulfil their potential.

Bullying of any kind is unacceptable at Hall Orchard. If bullying does occur, all incidents will be dealt with promptly and effectively in accordance with the school's Behaviour policy. The school actively implements its Behaviour policy and anti-bullying policy, and has clear pathways for reporting, which are known to all members of the school community. We celebrate diversity and promote cohesion within our community.

What is cyber bullying?

• Cyber bullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology.

• It can take many forms, but can go even further than face-to-face bullying by invading home and personal space and can target one or more people.

• It can take place across age groups and target pupils, staff and others.

• It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images including 'sexting'.

• It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyber bullying may be carried out in many ways, including:

• Threatening, intimidating or upsetting text messages;

• Threatening or embarrassing pictures and video clips via mobile phone cameras;

• Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;

• Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;

• Menacing or upsetting responses to someone in a chat-room;

• Unpleasant messages sent during instant messaging;

• Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook).

Sexting

'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media and/or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, Hall Orchard takes a pro-active approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'.

There are a number of definitions of 'sexting' but for the purposes of this policy sexting is simply defined as:

• Images or videos generated - by children under the age of 18, - or of children under the age of 18 that are of a sexual nature or are indecent.

• These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

The school recognises its duty of care to its young people who find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed. Our Computing Curriculum explicitly teaches the importance of not sharing personal information and images.

Roles and Responsibilities:

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they shall:

- Review this policy biannually and in response to any e-safety incident to ensure that: the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-Safety within the school. The Headteacher shall ensure that:

- E-Safety training throughout the school is planned, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents.
- All e-safety incidents are dealt with promptly and appropriately.

Computing Lead

Reporting to the Headteacher, the Computing Lead is responsible for the day-to-day delivery of e-Safety learning activities throughout the school. The Computing Lead shall:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Governing body on all e-Safety matters.
- Engage with parents and the school community on e-Safety matters at school and/or at home.
- Provide support with any e-safety issues raised via CPOMS.

IT Technical Support Staff

Reporting to the Headteacher, the IT Technical Support Staff are responsible for delivery of effective, secure and safe IT Solutions for the school. The Technical support staff are responsible for:

- Ensuring any technical e-Safety measures in school (e.g. Internet filtering software) are fit for purpose and operating correctly through liaison with the outside agencies.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-Safety coordinator(s) and Headteacher.

- Ensuring Anti-virus is fit-for-purpose, up to date and applied to all capable devices.

- Ensuring Windows/iOS (or other operating system) updates are regularly monitored and devices updated as appropriate.

- Ensuring Passwords are applied correctly to all staff. Passwords for staff shall be regularly updated.

- Ensuring staff use encrypted laptops and computers and save documents and pictures to the school system.

- Monitoring and reporting of documents stored on internal systems, internet and email use for both staff and pupils and report any inappropriate action to the Headteacher.

- Ensuring the IT System Administrator password is changed regularly.

All Staff

Staff shall ensure that:

• All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher and the Computing Lead.

• Any e-Safety incident is reported via CPOMS.

• Use of technology in lessons, in particular the use of the internet, has been checked to ensure age appropriate content.

• Where appropriate, staff should ensure they feel adequately informed to be able to deliver e-Safety lessons to students.

All Pupils

Pupils are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy.

Through regular e-Safety education, all pupils should:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Similarly, all students will be fully aware of how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will support parents to help them gain the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and workshops, the school will keep parents up to date with new and emerging e-Safety risks, and will involve parents in strategies to ensure that students are empowered to make informed decisions. It shall be made clear to parents that the school needs rules in place to ensure that their child can be properly safeguarded.

Safe Use

Internet – Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide students with quality Internet access as part of their learning experience. Students must request permission before using the internet and only access sites approved by staff. The school uses filters and firewalls to prevent pupils from accessing inappropriate material on the school network which is constantly reviewed to safeguard our pupils. Some inappropriate material will bypass these safeguarding procedures. However, the school

priorities teaching pupils across the school in how to deal effectively with inappropriate content by showing a teacher immediately; the teacher will then report this to the IT Technical Support Staff.

In Key Stage 1, access to the Internet shall be by adult demonstration with occasional directly supervised access to specific, approved online materials.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted unless permission has been granted by the Headteacher. Staff are not permitted to email students.

Photos and videos – All parents must sign a photo/video release slip when their child joins the school. Photos or videos taken on a device for curriculum purposes must be transferred to our school's network and then removed the same day. A device which is being used during residential trips must be kept in a secure area and photos and videos downloaded at the end of the trip.

System - USB storage devices may not be used. School laptops and computers are password protected. School laptops and documentation stored on the system drives will be monitored by the school. Staff shall not use any personal device (e.g. personal cameras/phones) to store pupil information including photos/videos.

Website - The contact details on the website are the school's address, e-mail and telephone number. Staff or pupils' personal information shall not be published. The Headteacher or nominee shall take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs that include pupils will be selected carefully. Pupils' full names shall not be used anywhere on the website including in blogs, forums or wikis, particularly in association with photographs. All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use.

Social Networking – there are many social networking services available, however Hall Orchard do not permit the use of any external social media site in school unless short-term access is required for a specific educational project. This does not include blogs, wikis or forums accessed via any online platform. Content/comments posted on these sites shall be monitored by the school staff and IT Support.

Note: Hall Orchard believes our pupils should adhere to the age of consent rules when opening a social media account (users should be a minimum of 13 years of age) and teaching of these rules will be given in e-Safety lessons.

School staff must take care to protect their privacy and protect themselves from risk of allegations in relation to inappropriate relationships and cyber-bullying. Staff must not have any unauthorised contact or accept 'friend' requests through social media with any pupil (including former pupils and/or those who attend other schools) unless they are family members.

If employed by (or associated with) the school, it is crucial to refrain from referring to school matters, whether this is regarding information about a child, another member of the school team or, in the case of staff who are also parents of the school, their experiences of the school as a parent. Staff must exercise caution when having contact online through social media with parents so as not to compromise the school's reputation or school information. This includes staff contacting other staff in any sort of public domain which can be seen by other members of the public (e.g. parents or children).

Mobile technologies - Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative working environment and thus open to risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

- Pupils are allowed to bring personal mobile devices / phones to school but they must be switched off whilst in school. Smart watches brought to school must be disconnected from the internet. We reserve the right to confiscate these devices if they are used inappropriately. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Incidents & Complaints

Any e-Safety incident is to be brought to the immediate attention of the Headteacher via CPOMS. 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. Sanctions within the school include: – interview/counselling by class teacher / Headteacher; – informing parents or carers; removal of Internet or computer access for a period.

Training and Curriculum – The Headteacher and Computing Lead are responsible for staying up to date with new information/research pertaining to e-Safety. Hall Orchard will have an annual programme of training which is suitable to the audience. E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff shall ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Teaching and Learning

Children shall be taught about Internet safety using materials from CEOP and in accordance with the Computing curriculum. This will take place within Computing and PSHE lessons.

Pupils shall be informed that network and Internet use is monitored. E-Safety rules will be discussed with all pupils at the start of each year and regularly referred to across the curriculum. Staff may only create blogs, wikis or forums in order to communicate with pupils using the school's website or other systems approved by the Headteacher.

Pupils shall be supervised at all times when using the internet. They are given clear objectives and must ask permission before accessing different sites. All websites used in lessons, are checked by staff. Prompt action shall be taken if pupils encounter inappropriate material. Both staff and pupils are taught to switch off the monitor and pupils must report the incident immediately to a member of staff. Staff must record the website address and report it to the IT Support, Computing Lead and/or Headteacher. If necessary, a discussion will take place with the pupil and parents/carers shall be informed.

Pupils shall be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Important aspects surrounding the laws on copyright of material will also be covered.

Pupils shall be taught:

- The importance of Digital Citizenship (respect, courtesy and responsibility) when communicating with others online.
- Never to give out personal details of any kind which may identify them or their location (i.e. full name, address, mobile/home phone numbers, school details, IM/email address, and specific hobbies/interests).
- To deny access to unknown individuals and how to block unwanted communications. Students are told to invite known friends only and deny access to others.
- The importance of passwords and other levels of security such as Anti-Virus & Malware protection.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy. In addition, pupils will be taught about the importance of copyright laws and illegal use of information from the internet.
- Not to place personal photos on any social network space provided in the school learning platform.
- The use of social network spaces outside school is inappropriate for primary aged pupils, parents / carers will also be advised.
- Not to share passwords or use another's account on any digital system. Staff shall model this behaviour by only using their own school accounts whenever possible.
- To be cautious about the information given by others on sites, for example users not being who they say they are.
- To avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- To set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- To be wary about publishing specific and detailed private thoughts online.
- To report any incidents of bullying to the school.
- Clear guidance on how to seek help and support if they experience an incident on the internet.

Further information can be found from the following sources:

- The Think u Know website by Child Exploitation and Online Protection (CEOP) website www.thinkuknow.co.uk/parents or www.thinkuknow.co.uk/teachers
- Use www.pegi.com to check suitability for all games (E.g. PlayStation, Wii, Xbox etc)
- NSPCC - www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- Childnet - http://www.childnet.com/
- Google's informative safety center has a simple step by step guide: www.google.com/familysafety/tools

Policy monitored by IT Support, Headteacher, Computing Lead, Governors.

Written: January 2020

Review date: January 2022