**Policy Number: 7h**

# Policy Title: Online Safety Policy - Whole School Policy including EYFS and Boarding

**Author: Paddy Tyrer and Suzie Brown**

**Last updated: September 2022**

This Policy has been developed using the Department for Education Guidance on Teaching Online Safety in School (June 2019). It should be read in conjunction with the Discipline, Behaviour, Sanctions and Rewards Policy, Safeguarding and Child Protection Policy, Anti-Bullying Strategy and ICT Acceptable Use Policy for Staff, as well as the links to useful guidance to be found on the school website in the section entitled Staying Safe Online. This policy aims to provide some guidelines as to what the school expects from the staff, pupils and parents.

## 1. BACKGROUND

1.1 As a school, Hall Grove embraces technology and is fully supportive of the provision it gives to enhance a child's learning experience. There are, however, dangers associated with technology and, more specifically, the Internet. We seek to ensure that pupils understand how to behave and stay safe online by providing them with the knowledge needed to make best use of the internet and technology in a safe, considered and respectful way.

1.2 Hall Grove teaches online safety in a variety of ways, building it into existing lessons across the curriculum, within specific online safety lessons and in whole school settings such as assemblies or talks by guest speakers. Teaching is always age appropriate and tailored to the development stage of the children. External experts run pupil, parent and staff Online Safety workshops regularly.

1.3 The school will take all reasonable precautions to ensure Online Safety at school. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it can be difficult for schools to stay up to date with the latest advances and the potential threats associated with them. Hall Grove uses a number of control measures but it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

1.4 Given the pervasive nature of technology in today's society and the ready access children of all ages have to it at home, parents are strongly advised to keep up to date with developments and are urged to monitor their child's usage of technology out of school. A number of useful resources are listed on the school website under Staying Safe online.

## 2. STAFF RESPONSIBILITIES

2.1 Online Safety is a pervasive topic across all subjects. All staff are responsible for promoting and supporting safe behaviour in their classrooms and for following Online Safety procedures. Staff should also be aware of their personal responsibilities to protect the security and confidentiality of the school network.

2.2 It is the duty of all staff to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

2.3 Maintain password security. Passwords should not be shared with any other member of the school community, nor should they be written down. When unattended, computers must be logged off or locked down.

2.4 Any accidental access of inappropriate material on the Internet should be reported to the Network Manager immediately. The school reserves the right to examine internet access logs from any computer in the school and staff laptops or other devices issued by the school. The school cannot accept liability for material accessed, or any consequences of Internet access.

2.5 Emails from suspicious sources should not be opened. These should be reported to the Network Manager. Software should not be downloaded unless the source can be trusted and the member of staff has checked that there is no infringement of licensing laws.

2.6 Staff are offered advice regarding the use of social media. All staff are required to read and sign the ICT Acceptable Use Policy for Staff document.

2.7 It is important that ALL staff and volunteers are alert to the potential risks children may be exposed to, and steps can be taken to mitigate the risk of this occurring, with specific reference to:

a. Content:- e.g. exposure to age-inappropriate material, inaccurate or misleading information, socially unacceptable material (e.g. inciting violence, hate or intolerance) and illegal material (including images of child abuse or terrorist or extremist ideologies);
b. Contact:- e.g. grooming using communication technologies leading to inappropriate behaviour or abuse;
c. Commerce:- e.g. exposure to inappropriate advertising, online gambling, identity theft, and financial scams;
d. Culture:- e.g. bullying via websites, mobile phones or other communication technologies, or inappropriate downloading of copyright materials (i.e. music, films, images; exposure to inappropriate advertising, online gambling, identity theft, and financial scams;

2.8 Staff are not permitted to have online contact with pupils on social media sites (for example Facebook and Instagram). The school provides advice to staff regarding their personal online activity and has strict rules regarding online contact and electronic communication with pupils. Staff found to be in breach of these rules may be subject to disciplinary action or child protection investigation. More information can be found in Staff Handbook.

## 3. CONTROL MEASURES

3.1 IT is provided to help enhance the children's learning and staff are suitably trained to ensure all opportunities are taken. The Network Manager has access to all pupils' accounts and are able to closely monitor pupil activity, both online and off.

3.2 The school has a sophisticated firewall system which blocks sites deemed inappropriate and searches the content of a website before allowing access. (Watchguard Firewall / iBoss Web Filtering) (iPads – additional content filtering software installed). All IT Suite PCs are also protected with NetSupport DNA montioring. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Online Safety coordinator. In addition, all Chromebooks have the Lightspeed Systems filter installed along with NetSupport DNA, which monitors all internet traffic from any network that the Chromebook is connected to, either in school or externally when being used at home. All Chromebook devices are registered and managed with Lightspeed MDM.

3.3 No child has a personal school email address. All social networking sites are blocked. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. Students must always be supervised in IT suites and in classrooms where laptops or iPads are in use.

3.4 Whilst all staff incorporate Online Safety into their teaching, it is also covered in Computing and PSHE lessons and in assemblies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.5 The Network Manager liaises closely with the Section Leaders as and when issues arise. The Headmaster is kept fully abreast of any issues regarding the inappropriate use of IT and ultimately decides any sanctions which are deemed necessary.

3.6 Throughout the school staff monitor children closely when using computers or other forms of technology. No unsupervised use of computers is permitted.

3.7 When a child is registered at Hall Grove the parents sign to give consent for photos to be taken and used where appropriate on the website and in school publications.

## 4. MOBILE PHONES

4.1 Children are NOT allowed mobile phones or electronic devices with any form of messaging capability (such as iPods) either at school or on a school trip without the express permission of the Headmaster.

4.2 If permission is granted, the device is only to be used with the permission of the trip leader to contact family via text or phone. Access to social networking, the Internet and email is strictly prohibited when children are under the care of school staff.

## 5. THE ROLE OF PARENTS

5.1 Parents should be aware that all social media sites are 13+ and therefore younger children should not be allowed to use them. Parents are advised to keep abreast of issues involving IT, the Internet, social media and mobile phones and to monitor their child's online activity. Advice and useful websites for parents are listed on the school website section entitled Staying Safe Online. Whilst there are many positives with technology, it is advisable for parents to be aware of the risks involved. Modern advice suggests it is advisable for parents to embrace technology – it is a massive part of children's lives and the world they are growing up in.

5.2 It is the responsibility of the school and parents together to educate their children to be aware of the dangers of social media and the Internet. There are two main areas of risk when children use social networking and gaming sites:

a. The child creates or posts inappropriate, offensive or even illegal material – this can lead to trouble with friends, school or even the police. It is very difficult to take back something that may later be regretted.
b. Children can put too much personal information on these sites, and are often unaware of ways they can protect themselves. This can lead to approaches from adults with an inappropriate interest in young people.

5.3 With social media and gaming, parents are encouraged to:

a. Try and be positive and strike a balance between allowing children space and privacy yet ensuring they are aware of the risks.
b. Make sure children know how to protect themselves on social media and when using interactive gaming sites. Parents may like to remind their children to keep passwords safe and to check the privacy settings on their accounts.
c. Most children will want to include a photo of some sort to form part of their profile – they should be encouraged to think about the sort of photo posted and consider the fact that photos can easily be copied, shared, changed or used elsewhere.
d. Discuss the sorts of posts which might be appropriate and those which are not, particularly when discussing other people. What may start or be intended as a joke can quickly escalate and lead to gossip and pain which cannot be taken back.
e. It is crucial children feel able to discuss inappropriate or illegal activity they might come across online.

5.4 If a parent has concerns regarding Online Safety, they should in the first instance inform their child's form teacher who will ALWAYS discuss the issue with the Section Leader. The school takes such issues very seriously and the Section Leader will talk to the Head of Pastoral Care or Headmaster if it is deemed necessary. If a parent wishes to make a complaint about Online Safety, they should follow the school's Complaints Procedure as outlined on the website.

## 6. BOARDING

Boarders are subject to the same rules as day pupils. They are given access to the computers in the Admiral Room but only under supervision of Boarding staff.

This Online Safety Policy will be reviewed regularly in the light of any significant new developments in the use of technologies, new threats to online safety or specific incidents that have taken place.