Whole School Hall Grove E Safety Policy

Also see Discipline, Behaviour, Rewards and Sanctions Policy, Safeguarding, Anti-Bullying Strategy, Mobile Phone Policy and ICT Acceptable Use Policy for Staff.

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. This policy aims to give some basic guidelines as to what the school expects from the pupils and parents.

The school will take all reasonable precautions to ensure E Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

External experts run pupil, parent and staff E safety workshops regularly. (Karl Hopwood – May 2015)

This policy links closely with those on behaviour, safeguarding, data protection and bullying.

- 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.

Staff Responsibilities

- All staff are responsible for promoting and supporting safe behaviour in their classrooms and for following E-Safety procedures. Staff should also be aware of their personal responsibilities to protect the security and confidentiality of the school network.
- 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.
- 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.
- 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.
- 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.
- 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.

Control Measures

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

- The school has a sophisticated firewall system which blocks sites deemed inappropriate and searches the content of a website before allowing access. (Firewall: Equiinet Cache Pilot using Protex Web Filtering) (Ipads – additional content filtering software installed). If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

- 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 ICT suites and in classrooms where laptops or iPads are in use.
- Internet safety is covered in IT and PSHE lessons and there are regular reminders from the ICT Coordinator, form staff and in assemblies.
- The Network Manager liaises closely with the Heads of Section as and when issues arise. The Headmaster is kept fully abreast of any issues regarding the inappropriate use of ICT and ultimately decides any sanctions, which are deemed necessary.
- Throughout the school staff monitor children closely when using computers or other forms of technology.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Phones

- 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.
- 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.

The role of parents and the school

- Parents are advised to keep abreast of issues involving ICT, the Internet, social media and mobile phones. Advice and useful websites for parents are listed on the school website.

- 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.
- It is the responsibility of the school and parents 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:
    1) 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.
    2) 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.
- With social media and gaming, parents are encouraged to:
    1) Try and be positive and strike a balance between allowing children space and privacy yet ensuring they are aware of the risks.
    2) 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.
    3) 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.
    4) 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.
    5) It is crucial children feel able to discuss inappropriate or illegal activity they might come across online.
- There are several very useful sites which can be used for parents to glean further information if required:
  www.childnet.com/blogsafety
  www.digizen.org/socialnetworking
  www.chatdanger.com

If a parent has concerns regarding e-safety, they should in the first instance inform their child's form teacher who will ALWAYS discuss the issue with the Head of Section. The school takes such issues very seriously and the Head of Section will talk to the Headmaster if he/she deems it necessary.

If a parent wishes to make a complaint about e-safety, he/she should follow the school's complaints procedure as outlined on the website.

This E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Written by TGJL Sept 2015
To be revised July 2016