Policy : Online Safety/Behaviour

Co-ordinator : J Whyte

Reviewed : September 2016

Next Review Date : September 2017

Rationale:

The potential that technology has to impact on the lives of all people increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming both the way schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in Holley Park. This policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents / carers, friends and the wider community) to be aware and to assist in this process.

Introduction

- The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these sites unfamiliar to the teacher.
  There is therefore the possibility that a pupil may access unsuitable material.
  The purpose of this policy is to:
- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our behaviour and school policies.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.
- At Holley Park Academy, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Policy and Leadership:

All at Holley Park Academy are committed to safeguarding children in our care. This policy has been developed by the Online Safety/ Computing Co-coordinator/School Designated Officer and the Senior Leadership Team in order to ensure that it truly reflects our robust and thorough approach to safeguarding. This section outlines responsibilities of staff, leaders and stakeholders as well as all users of technology within school.

Responsibilities of the Online Safety Co-ordinator:

The Online Safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to Online Safety. The Online Safety coordinator:

- Is responsible for reviewing the school Online Safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
- Provides training and advice for staff, pupils and parents / carers.
- Liaises with the Local Authority where necessary.
- Liaises with school ICT technical support to ensure that internet access is appropriately filtered.
- Reports regularly to Senior Leadership Team.
- Receives appropriate training and support to fulfill their role.

Responsibilities of Governors:

Governors are responsible for ensuring that this policy in reviewed and enforced effectively.

Responsibilities of Head Teacher:

The head teacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety is delegated to the Online Safety Co-ordinator. The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Responsibilities of classroom based staff:

Teaching and Support Staff are 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 and they participate in Online Safety training for all staff.
- They have read, understood and signed the school's Acceptable Use Policy for staff.
- They report any suspected misuse or problem to the Online Safety Co-ordinator.
- Any digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- Ensure Online Safety issues are embedded in the curriculum and other school activities.

Responsibilities of the ICT Technician:

The ICT Technician is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Users may only access the school's networks through a properly enforced password protection policy.
- Ensuring that filtering is effective.
- Shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

Policy Scope:

This 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 school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the

behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Acceptable Use Policies:

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems. Acceptable use policies are reviewed and amended annually as needed in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents. For children in EYFS and KS1 parents may sign on behalf of their children. Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy. Parents sign once when their child enters the school. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year. Induction policies for all members of the school community include this guidance.

Whole School approach and links to other policies:

This policy has strong links to other school policies as follows:
Core Computing policy.
Anti-bullying policy.
PSHE policy.
Child Protection: Safeguarding children electronically is an important aspect of Online Safety. The Online Safety policy forms a part of the school's Child Protection policy.
Cyber-Bullying Policy.
Keeping Children Safe in Education 2016
Behaviour policy: Linking to positive strategies for encouraging Online Safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions:

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images (illegal - The Protection of Children Act 1978).**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).**
- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).**
- **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).**
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business.
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).

- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour management procedures.

Use of hand held technology (personal phones and hand held devices):

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. Devices should only be used by members of staff in areas not accessed by pupils. Mobile phones should be kept in a closed cupboard and on silent during the school day.
- Pupils in Year 6 are permitted to bring their personal hand held devices into school with the signed agreement of parents / carers but they should be switched off during school times. Parents / carers are responsible for the devices whilst in school.

Wearable Technology

- At Holley Park Academy we have a 'wearable technology' policy. Children are not permitted to wear technology such as the 'Apple watch' and other wearable devices which can send and receive pictures, videos, texts and messages.
- If a child is found to have wearable technology then this will be treated in the same manner as using a mobile phone within school.

Email:

Access to email is provided for all staff in school on their desktop. These official school email services may be regarded as safe and secure and are monitored.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

How will email be managed?

- Whole class or teacher email addresses will be used in Holley Park Academy for communication outside of the school by children.
- Pupils may only use approved email or blogging accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.
- Staff should not communicate with pupils via email.

Use of digital and video images:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use,

sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission. Parent's permission is sought at the start of each year to take photographs and video for educational purpose only.

Use of web-based publication tools:

Our school has its own website for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils). Only pupil's first names are used on the website, and only then when necessary. Photographs can be used (parental consent for this is obtained at the start of each school year).

Professional standards for staff communication:

In all aspects of their work in our school, teachers abide by the Teachers' Standards as described by the DfE. Teachers translate these standards appropriately for all matters relating to Online Safety. Any digital communication between staff and parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications. Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

How will social networking, social media and personal publishing be managed?

- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.
- Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Teachers cannot under any circumstances mention any references to their working lives on any social media.
- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

How will Internet access be authorised?

- We allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not.
- Authorisation is as individuals and usage is fully supervised. Normally all pupils will be granted Internet access.

- Parental permission is required via Acceptable Use Agreement for Internet access in all cases as new pupils join Holley Park.
- All staff must read and sign the Code of Conduct before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

Filtering:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities:

The day-to-day responsibility for the management of the school's filtering policy is held by the ICT technician and Online Safety Co-ordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system. All users have a responsibility to report immediately to class teachers / Online Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked. Users must not attempt to use any programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / training / awareness:

Pupils are made aware of the importance of filtering systems through the school's Online Safety Education Program. Staff users will be made aware of the filtering systems through:

- Signing the AUP (a part of their induction process)
- Briefing in staff meetings, training days, etc. (from time to time and on-going).

Parents / carers will be informed of the school's filtering policy through the Acceptable Use agreement and through Online Safety awareness sessions.

Monitoring:

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

How will information systems security be maintained?

- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.

Online Safety education:

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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. Online Safety education will be provided in the following ways:

- A planned Online Safety program should be provided as part of Computing, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Use of the resources on CEOP's Think U Know site as a basis for our Online Safety education.
- Learning opportunities for Online Safety are built into the Safe and Acceptable Use strand of the Holley Park Academy Curriculum Entitlement for Computing.

- Key Online Safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- 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 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Information literacy:

Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

- Checking the likely validity of the URL (web address).
- Cross checking references (can they find the same information on other sites)?
- Checking the pedigree of the compilers / owners of the website.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require.

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning. Pupils play a part in monitoring this policy.

Parent and carer awareness raising:

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Parent's evenings.
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others.
- Use of outside agencies to support parents.