St Hilda's School
HARPENDEN
Caring, Curious & Confident

E-Safety & Computing Acceptance Usage Policy

Important Note

Unless otherwise stated, all Policies of St Hilda's School apply to the school in its entirety. This comprises all staff and pupils in the Early Years Foundation Stage (EYFS), the Junior School (Key Stage 1) and the Senior School (Key Stage 2).

REVIEW DATE: **APRIL 2019**

REVIEWED BY: **Dan Sayers (Headmaster)**

SIGNED BY: D. J. Sayers.

DATED: **30.04.19**

INTRODUCTION

This policy should be read in conjunction with the Mobile Phone Usage Policy.

RATIONALE

As a school working with local, national and international communities, Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children and adults. Consequently, schools need to build in the use of these technologies in order to arm pupils with the skills to access life-long learning and employment.

Computing covers a wide range of resources, including web-based and mobile learning. It is important to recognise the constant and fast paced evolution of Computing within society as a whole.

Whilst exciting and beneficial both in and out of the context of education, much of Computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

St Hilda's School recognises its responsibility to educate pupils on e-safety issues; this includes teaching pupils the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, both within and beyond the context of the classroom.

This policy (which includes the Acceptable Use Agreement applicable to all staff, Governors, visitors and pupils) is inclusive of both wired and wireless; technologies provided by the school (such as PCs, laptops, whiteboards, digital video equipment, ipads etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, ipads, mobile phones, camera phones and portable media players etc).

ROLES AND RESPONSIBILITIES

As e-safety is an important aspect of strategic leadership within the school, the Governors have ultimate responsibility to ensure that the policy and practices here described are embedded and monitored. This responsibility is delegated to the Headmaster. Any additional permission given by the Headmaster must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The Headmaster (who is the Designated Senior Person), the Senior Management Team, the Business Manager and the Head of Computing have day to day responsibility for ensuring that these policies are upheld by all members of the school community and that all are made aware of the implications of the policies. It is the role of the Headmaster and the Business Manager to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and the Local Authority Safeguarding Children Board.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- The school ensures that staff receive regular information and training on e-safety issues in the form of full staff meetings and memos
- New staff receive information on the school's Acceptable Use Agreements as part of their induction through their employee handbook
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas

E-SAFETY IN THE CURRICULUM

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within the school's curriculum and we continually look for new opportunities to promote e-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete Computing lessons to teach about e-safety

- Educating pupils on the dangers of technologies that may be encountered outside school may also be done informally when opportunities arise

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities

- Pupils are made aware of the impact of online bullying and know they can seek help from their Form Teacher, Mentor and "worry box", if they are affected by these issues.

- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the Computing curriculum

DATA SECURITY

The accessing and appropriate use of school data is a matter that the school takes very seriously. Staff are made aware of their responsibility when accessing school data. The level of access is determined by the Headmaster.

MANAGING THE INTERNET

The internet is an open communication medium, available to all at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

INFRASTRUCTURE

- School internet access is controlled through a web filtering service
- The school also employs some additional web filtering.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform the Business Manager and Headmaster

- It is the responsibility of the school, by delegation to technical support, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first

MANAGING OTHER WEB TECHNOLOGIES

The school acknowledges that, if used responsibly both outside and within an educational context, web technologies can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage pupils to think carefully about the way that information can be added to and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught 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
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Pupils are asked to report any incidents of cyber bullying to the school

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, well-known device with possible internet access and thus open up 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. St Hilda's School chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use
- Pupils are not allowed to bring personal mobile devices/phones to school
- 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

(Please refer to the Mobile Phone Usage Policy)

MANAGING EMAIL

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits, including direct written contact between schools on different projects (be they staff-based or pupil-based) within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. Pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business
- **Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses**
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school paper
- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes
- The following pupils have their own individual school issued accounts: Forms IV-VI
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail
- Staff must inform the Business Manager and Headmaster if they receive an offensive e-mail
- Pupils are introduced to email as part of the Computing Scheme of Work

TAKING OF IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and can therefore be misused. It should be remembered that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- on the school's Facebook page
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

STORAGE OF IMAGES

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) unless for an assignment or immediate transfer to the staff shared area
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school computers
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school, unless they are deemed necessary for historical/archive purposes

MISUSE AND INFRINGEMENTS

Complaints

- Complaints relating to e-safety should be made to the Business Manager or Headmaster
- All incidents will be logged and followed up
- Complaints of a child protection nature must be dealt with in accordance with Safeguarding/Child Protection policies and reported in accordance with the policy
- Pupils and parents will be informed of the complaints procedure

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headmaster
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headmaster. Depending on the seriousness the offence and outcome of the investigation, the school may invoke immediate suspension, possibly leading to dismissal and the involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct

EQUAL OPPORTUNITIES

Pupils with additional needs

Teaching staff are aware that some pupils may require additional teaching, including reminders, prompts and further explanations to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned in accordance with any specific learning needs

PARENTAL INVOLVEMENT

The school believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits related to Computing, as well as the associated risks.

- Parents are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website)

- The school disseminates information to parents relating to e-safety where appropriate in the form of

    - Information sessions
    - Posters

- Parents are advised that the use of social network spaces outside school is inappropriate for under the age of 13 children.

- Parents are expected to reinforce the guidance from school when using technologies at home. The school is not responsible for communications between pupils outside school through social networking sites.

REGULATION OF INVESTIGATORY POWERS ACT 2000

Ancillary to their provision of Computing facilities, the Governors asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

This policy will be reviewed annually, by the Senior Management Team, in line with the school's review schedule for policies.