St Hilda's School
HARPENDEN
Caring, Curious & Confident

ONLINE SAFETY & COMPUTING ACCEPTABLE USAGE POLICY

Name of Policy	Online Safety & Computing Acceptable Usage Policy
Reviewed by	Dan Sayers Faye Smith
Review Date	October 2026
Next Review Date	October 2028
To be Read in Conjunction with	• Taking, Storing and Using Images of Children Policy • Mobile Phone Usage Policy • Internet and Email Acceptable Use Policy • Safeguarding (Child Protection) Policy
Legislation Referenced	Regulation of Investigatory Powers Act 2000

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).

CONTENTS

1. INTRODUCTION
2. RATIONALE
3. ROLES AND RESPONSIBILITIES
4. ONLINE SAFETY SKILLS DEVELOPMENT FOR STAFF
5. ONLINE SAFETY IN THE CURRICULUM
6. DATA SECURITY
7. MANAGING THE INTERNET
8. INFRASTRUCTURE
9. MANAGING OTHER WEB TECHNOLOGIES
10. MOBILE TECHNOLOGIES
11. GOOGLE ACCOUNTS AND GOOGLE CLASSROOM
12. MANAGING EMAIL
13. TAKING OF IMAGES AND FILM
14. STORAGE OF IMAGES
15. MISUSE AND INFRINGEMENT
    - 15.1 Complaints
    - 15.2 Inappropriate material
16. EQUAL OPPORTUNITIES
17. PARENTAL INVOLVEMENT
18. REGULATION OF INVESTIGATORY POWERS ACT 2000

1. INTRODUCTION

This policy should be read in conjunction with the Safeguarding (Child Protection) Policy, Mobile Phone Usage Policy, the Internet and Email Acceptable Use Policy and the Taking, Storing and Using Images Policy.

2. RATIONALE

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.

St Hilda's recognises that its pupils may, in situations outside of school, have unfettered access to the internet through smart devices. Technology and the platforms available, and the safeguarding risks and harms related to it, evolve, and change rapidly.

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

This includes understanding the safe use of, and risks posed by, emerging and developing technologies, including Artificial Intelligence, as well as being alert to the risks of online scams. In relation in particular to generative AI, further guidance may be found within the DfE guidance at: https://www.gov.uk/government/publications/generative-ai-product-safety-standards.

This policy is inclusive of wired and wireless; technologies provided by the school (such as PCs, laptops, Chrome books, 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).

3. ROLES AND RESPONSIBILITIES

As online 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 Headteacher.

The Headteacher, 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 Headteacher 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.

Filtering and Monitoring

St Hilda's ensures that appropriate firewall protection is in place to safeguard pupils from potentially harmful or inappropriate online material. St Hilda's ensures that it has the appropriate level of security protection in place in order to safeguard systems, staff and pupils. The procedures in place

are regularly reviewed to ensure effectiveness and to keep up with ever evolving cyber-crime technologies. Training is also provided to all staff to ensure awareness.

St Hilda's complies with the Department for Education's Filtering and Monitoring Standards. St Hilda's has appropriate filtering and monitoring systems in place and conducts twice-yearly reviews of their effectiveness of these systems. Records are kept of all results of the filtering and monitoring checks, and results are reviewed by the DSL once a week.

4. ONLINE SAFETY SKILLS DEVELOPMENT FOR STAFF

- The school ensures that staff receive regular information and training, including updates, on online safety issues (this includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) and cyber security.
- New staff receive information on the school's Acceptable Use Agreements as part of their induction .
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of online 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 online safety activities and awareness within their curriculum areas.

5. ONLINE SAFETY IN THE CURRICULUM

We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within the school's curriculum, and we continually look for new opportunities to promote online safety. We regularly monitor and assess our pupils' understanding of online 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 or Mentor if they are affected by these issues.
- Pupils are 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/Thinkyouknow 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.

Pupils and staff are made aware of the four main areas of risk regarding online safety: content, contact, conduct and commerce.

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

- Contact: harmful interaction with others, such as peer to peer pressure, grooming and exploitation.
- Conduct: online behaviour that increases the likelihood of, or causes, harm.
- Commerce: risks such as online gambling; phishing etc.

6. 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.

7. MANAGING THE INTERNET

The internet is an open communication medium, available to all at all times. Whenever any inappropriate use is detected – either internally or identified by the Schools web safety provider - 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, supervise this work and supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or software from other sources.
- During Homework Club (or at other similar times), the supervising adult is able to view live all internet searches being made. The screens of all pupils should be displayed on the smartboard in the classroom to both monitor and deter inappropriate searches.

8. INFRASTRUCTURE

- School internet access is controlled through a specific web filtering service. Care should be taken to avoid "over-blocking" that leads to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Staff and pupils are aware that school-based email and internet activity is monitored.
- 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.

9. 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 online 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.

10. MOBILE TECHNOLOGIES

The School has a specific **Mobile Phone Usage Policy** which should be considered in conjunction with this policy, and can be summarised as follows:

Use of mobile phones / smart technology by pupils

- St Hilda's School is phone-free by default. Pupils are not permitted to have mobile phones, or other forms of smart technology, whilst at School.
- Pupils in Form VI who walk to school unaccompanied by an adult are permitted to bring a non-Internet enabled 'brick' phone for the purposes of being contactable during their travel to and/or from school. These must be turned off at the school gate upon arrival, handed in to the school office for the day, collected at home time and turned on once off-site.
- There may be exceptional circumstances in which adjustments are made to allow a pupil to have access to a mobile phone or other smart technology device during the school day, for example if needed for medical monitoring. Each case will be assessed on its own merits and the permitted use of a device will be proportionate to the circumstances and individual need.

Use of mobile phones / smart technology by staff

- Staff are not allowed to use their personal mobile phones during the School day when in the presence of pupils.
- As an exception to this, personal mobile phones may be used for short instances solely for allowing access to school online systems which require multi-factor authentication.
- The School mobile phone may be used for the sole purpose of School business, for example the taking of photographs for displays or for School social media updates.

11. GOOGLE ACCOUNTS AND GOOGLE CLASSROOM

Google accounts are created for children in Forms II-VI and for teaching staff. Google Classroom is used as an online teaching platform for Forms III-VI.

- All children are issued with an individual username and a school issued password.
- All children are taught they are not to change the password without consent from the Head of Computing.

- Permission is sought from parents before the issue of a Google Account.
- Children are reminded of the Computing Agreements guidelines they sign at the beginning of each academic year.
- Children are reminded of suitable content for sending messages to teachers and that Google Classroom is to only be used for school purposes.

12. MANAGING EMAIL

The use of email within most schools is an essential means of communication for both staff and pupils. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. Pupils have experience 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.

13. TAKING OF IMAGES AND FILM

The School has a specific policy on **Taking, Storing and Using Images of Children** which should be read in conjunction with this policy. The written consent of parents (on behalf of pupils) to store and publish images of individual pupils or their work is obtained when a pupil joins the school. Parents may withdraw permission, in writing, at any time. All images will be deleted from the school website news pages and social media accounts, once the pupil leaves the School.

Pupils' full names will not be published alongside their image and vice versa.

14. 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.

15. MISUSE AND INFRINGEMENTS

15.1 Complaints

- Complaints relating to online safety should be made to the Business Manager or Headteacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with Safeguarding policies and reported in accordance with the policy.

15.2 Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported to the Headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher. Depending on the seriousness of 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.

16. 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 online safety issues.

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

17. PARENTAL INVOLVEMENT

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

- Parents/carers are advised that the use of social network sites is inappropriate, and in many cases prohibited, for children under the age of 13.
- Parents/ carers 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.

18. REGULATION OF INVESTIGATORY POWERS ACT 2000

The Proprietor reserves the right to monitor and inspect any computer or telephonic communications systems used by staff where there are grounds to suspect that such facilities are being, or may have been, misused.

This policy will be reviewed at least every two years by the Senior Management Team, in line with the school's review schedule for policies.