



Online Safety Policy

Approved by the LGB	September 2023
Next review due by	September 2024
Frequency	Annually

Our School Vision:

We believe every child has the right to be a successful and confident citizen who is able to make a positive contribution to the world they live in.

Our motto is 'Learning today, to make a difference tomorrow'

Our School Values:

Our School Values were updated following a consultation process with our stakeholders. The following table outlines ways in which a child might demonstrate our 4 core values.

<p>Compassion - we show kindness and understanding to everyone</p> <p>We show kindness to one another.</p> <p>We help one another.</p> <p>When someone is feeling hurt or sad, we try to make them feel better.</p> <p>We use kind words</p>	<p>Responsibility - we think about the impact of our actions.</p> <p>We make good choices about our behaviour. We think about how actions affect others.</p> <p>We look after our own and other people's property. We care for our environment</p>
<p>Courage - we are brave and believe we can We are not afraid to take risks or make mistakes.</p> <p>We will have a go at something new.</p> <p>We do not give up when we find something difficult.</p> <p>We will try things that we may be a little afraid to do.</p>	<p>Respect - we value everyone in all we do.</p> <p>We show good manners.</p> <p>We listen to others and their ideas.</p> <p>We treat each other as we would like to be treated. We celebrate differences and similarities between people.</p>

Our School Aims:

- Every member of our school community will understand, live and breathe each of our core values. to challenge, develop and nurture the 'Whole Child' so they are able to grow into confident, resilient and emotionally literate citizens of the future.
- Our children will receive a broad and balanced experience that progressively builds and deepens knowledge, understanding and skills across the curriculum.
- Our school community will work in partnership with parents, carers and governors.
- Our children will leave Hatchlands physically and mentally healthy and equipped with the skills to prepare them for their future.
- Our children will have high aspirations and no limits on their learning,
- All children will achieve, regardless of their background or starting points.

Our One School Rule:

We show kindness and respect to everyone.

T:\

Introduction

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using IT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed we must consider IT a life-skill.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. • Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Significant educational benefits result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries; • Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues; • Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfE.

Areas of risk online that are addressed through our curriculum:

- **Content** – Protecting pupils from illegal, inappropriate or harmful material. Empowering children to know who they can ask if they see anything that makes them feel uncomfortable. •
- **Contact** – Educating children on potential harmful online interaction with other users e.g. inappropriate advertisements, adults posing as children or young adults.
- **Conduct** – Promoting responsible use of the internet and positive personal online behaviour to avoid causing harm/upset to others.

The school Internet access will be designed expressly for pupil use. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval. Unsuitable websites will be filtered; therefore inaccessible to staff and pupils. The use of Internet derived materials by staff and by pupils complies with copyright law. Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work..

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
 - Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
 - Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all'

approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

T:\

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular::

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
 - Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the

internet see policy and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

5

T:\

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by recoding on CPOMS
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

Parents/carers

Parents/carers are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- National Online Safety APP
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

T:\

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in Information via our website through National Online Safety Resources]. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

7

T:\

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber bullying with their class groups, and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- The school sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. • In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

E-mail

- Email is an essential means of communication and has significant educational benefits. • Pupils are taught how to use e-mail within our comprehensive scheme of learning, teaching them how to send emails within a safe environment where only the pupils and the teachers have access.

Website management

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the website, particularly associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Chat and social networking

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will be taught the importance of personal safety when using social networking sites and chat rooms, games and apps.
- Pupils and parents should be made aware that some social networks, APPS and games are not appropriate for children of primary age.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

- Google Classroom will be used by staff and parent/carers to communicate and share class and school information. Access is controlled with passwords. Google Classroom will be used in the event of remote learning. (see Remote learning Policy)
- Staff in the Early Years will use the online assessment tool “Tapestry” to share attainment and achievement of pupils in nursery and reception with their parent/carers through photos, videos and written observations. Secure passwords are used for parent/carers to access this.

T:\

Additional technology used for communications

- Our policy is to discourage pupils from bringing mobile phones/smart watches to school. However, if parents wish their child to bring one for use before and after school, these must be handed in to the school office or class teacher for safe keeping during school hours.

Internet access

- All classes are timetabled to learn about computing. Children in KS1 and Ks2 have access to their own Chromebook.
- Most teachers have a laptop (or iPad) to use both at school and at home with internet access. • The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil’s access.
- Parents will be informed that pupils will be provided with supervised Internet access (see letter, pg 6).
- Parents will be asked to sign and return a consent form.

Risk assessments

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- All website access is filtered by Smoothwall
- The Headteacher and computing leaders will ensure that the online safety policy is implemented, and compliance with the policy monitored.

Filtering

- The school will work in partnership with the LA, IT support (Sweethaven Computers), DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. • The Computing Leaders will ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) by the DSL.
- Regular checks by Sweethaven Computers will ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering methods will be selected by the school in conjunction with the Trust and Sweethaven Computers and will be age and curriculum appropriate.

Pupils internet use

- Rules for Internet access will be posted near computer systems. (Page 5)
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

T:\

Staff internet Use

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the school e-safety policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter.
- Staff development in safe and responsible Internet use, and on school E-safety policy will be provided as required.

Photographic, video and audio technology

- Staff may use photographic or video technology to capture school trips and support appropriate curriculum activities. Staff must not use their own devices for this. • Videoconferencing and webcam use will be appropriately supervised for the pupil's age. • Images, audio and video taken on Ipad devices must be kept secure with the school's username and password.
- Images, audio and video taken on Ipad devices must be kept secure with the school's username and password.

Computing system security

- The school computing systems will be reviewed regularly with regard to security. • Virus protection will be installed and updated regularly.
- Use of memory sticks will be reviewed.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

Complaints regarding internet use

- Prompt action will be required if a complaint is made.
- The severity of the incident will determine the course of action.
- Responsibility for handling incidents will be delegated to the Designated Safeguarding Lead or Deputies.
- Parents and pupils will need to work in partnership with staff to resolve issues. • Sanctions available include: Informing parents or carers, removal of internet or computer access for a period.
- There may be occasions when the police must be contacted. Early contact could be made to

establish the legal position and discuss strategies.

- Any complaint about staff misuse must be referred to the Headteacher.

Google Classroom

'Where a pupil, class, group or small number of pupils need to self-isolate, or there is a local lockdown requiring pupils to remain at home, DfE expects schools to be able to immediately offer them access to remote education.' (www.gov.uk)

10

T:\

The purpose of our Google Classroom is to provide a safe and secure place to receive and share learning, and a place where we will be able to connect with school staff and classmates. In Google Classroom, school staff can assign work to the learners digitally, without paper. Google Classroom is accessible from any digital device with internet access and a web browser. Parents/carers can login and view the assignments that their children have been set, whether their child has completed and submitted them, and view feedback that they may have received.

Early Years will continue to use Tapestry to share and submit their learning however, any live interactions will take place via Google Classroom.

The Google Classroom agreement outlines what we expect of pupils and parents/carers during remote learning and what can be expected from us as a school. Much of this echoes our Core Values when in school and all of it is designed to help pupils benefit the most from remote learning and keep our whole community safe.

The following websites offer useful support:

[Childline](#) - for support

[UK Safer Internet Centre](#) - to report and remove harmful online content

[CEOP](#) - for advice on making a report about online abuse

In addition, the following sites are an excellent source of advice and information:






[Internet matters](#) - for support for parents and carers to keep their children safe online

[Net-aware](#) - for support for parents and careers from the NSPCC

[Parent info](#) - for support for parents and carers to keep their children safe online

[Thinkuknow](#) - for advice from the National Crime Agency to stay safe online

T:\

	I will be responsible by only using my own login and password.
	I will ask permission before entering any website.
	I will show respect by only looking at or deleting my own files.
	I will not tell other people on the internet personal things about me.
	I will not use Internet chat.



If I see anything I am unhappy with or I receive messages I do not like, I will have the **courage** to tell a teacher immediately.

I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of E-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or

12

T:\



I will be **responsible** by only using my own login and password.



I will ask permission before entering any website, unless my teacher has already approved that site







I will only e-mail people I know, or my teacher has approved. I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.



I will show **respect** by only looking at or deleting my own files.



I must not bring software, memory cards or USB sticks into school without permission

	I will be RESPONSIBLE and will not give my home address or phone number, or arrange to meet someone.
	I will not use Internet chat.
	The messages I send will be compassionate : polite and sensible.
	If I see anything I am unhappy with or I receive messages I do not like, I will have the courage to tell a teacher immediately.
<p>I know that the school may check my computer files and may monitor the Internet sites I visit.</p> <p>I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.</p>	

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of E-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.



Dear Parent/Carer

As part of your child's curriculum and the development of computing skills, we provide supervised access to the Internet. We believe that the use of the World Wide Web and email is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use, and sign and return the consent form so that your child may use the Internet at school.

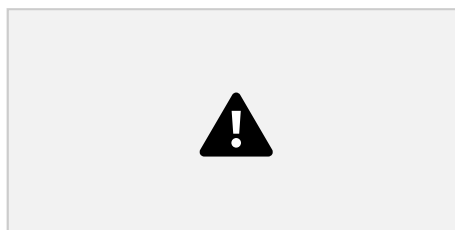
Our school Internet provider operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, Hatchlands cannot be held responsible for the nature or content of materials accessed through the Internet.

Hatchlands will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Headteacher



14

T:\



Responsible Internet Use

Please complete, sign and return to the school office

Pupil: _____ Class _____

Pupil's Agreement

I have read and understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Pupil's signature: _____ Date: _____

Parent/Carer's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent/Carer's signature: _____ Date: _____

Please print name: _____

Parent/Carer's Consent for Web Publication of Work

I agree that, if selected, my son/daughter's work may be published on the school website

Parent/Carer's signature: _____ Date: _____

T:\

15

Notes on the legal framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the headteacher. The Rules for Responsible Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act 1984/98 concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software. **The Telecommunications Act 1984** Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

References:

Brief introduction to dangers and legal aspects of the Internet.

www.bbc.co.uk/webwise/basics/user_01.shtml

List of useful law resources; see copyright and Internet sections.

<http://link.bubl.ac.uk/law>

HMSO: Full text of all UK legislation and purchase of paper copies.

www.legislation.hmso.gov.uk