Hillesley
PRIMARY SCHOOL

Our vision, based on our School's Christian values, is to provide a welcoming, nurturing environment for learning at the heart of our community. Together, we provide a solid foundation of growth, appreciating each child with their God-given uniqueness and individual needs, thus empowering them to become responsible and fulfilled members of society

Online Safety Policy

Approved by:	HILLESLEY PRIMARY SCHOOL GOVERNORS	**Date:** September 2023
Next review due by:	September 2024	

Contents

1. Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Hillesley Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership team to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with IT providers (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Behaviour in schools
- Filtering & Monitoring in schools
- Cyber security standards for schools and colleges
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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 include any issues arising around online safety at regular governor meetings, and monitor any online safety incidents provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Ensure that the school has appropriate filtering and monitoring systems in place, and review their effectiveness.
- Make sure that the staff are aware of the filtering and monitoring provisions in place, and that they understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training
- Ensure that the Governor responsible for Safeguarding will review the DfE's filtering and monitoring standards, and discuss with the DSL/service providers what needs to be done to support the school in meeting these standards
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and DDSL 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see appendix 4) 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
- Understanding the filtering and monitoring processes on school devices and school networks to keep pupils safe online and reviewing the effectiveness of these
- Working closely with IT providers and the Safeguarding Governor to understand, review and drive the rationale behind systems in place for filtering and monitoring, initiate regular checks and annual reviews
- Updating and delivering staff training on online safety, filtering and monitoring and cyber security (appendix 4 contains a self-audit for staff on online safety training needs)
- Cascading knowledge of risks and opportunities throughout the school community, e.g. via staff meetings, emails, newsletters.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety, filtering and monitoring in school to the governing board
- Carrying out an annual review of the school's approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks children face
- Ensuring a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

This list is not intended to be exhaustive.

3.4 The ICT management (School Administrator/GCC IT dept/Focus Networks/EXA)

The ICT management is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Maintaining filtering and monitoring systems
- Working closely with the school's DSL to monitor and review and improve filtering and monitoring approaches
- Providing filtering and monitoring reports to DSL/Safeguarding Governor
- Completing actions following concerns or checks to systems
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) 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 child protection policy, behaviour policy and anti-bullying policy

This list is not intended to be exhaustive.

3.5 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
- Understanding their responsibilities and those of others with regard to filtering and monitoring, including the importance of feeding back potential issues to the DSL

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents 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
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Pupils

Pupils are expected to:

- Read, understand and sign the acceptable use agreement

3.8 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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Visitors are expected to:

- Report any concerns, no matter how small, to the DSL

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, predominately in Computing/PSHE and RSE lessons:

In **Key Stage 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 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

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Educating parents about online safety

The school will raise parents' awareness of online safety in letters or other communications home, and in information via our website or remote learning platform. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings and meetings with Cyber Safety Officers.

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

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

6. Cyber-bullying

6.1 Definition

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.)

6.2 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.

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 pupils.

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, RSE and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also 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. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1& 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1& 2.

8. Pupils using mobile devices in school

Pupils **are not permitted to** bring mobile devices into school.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Using 2-Factor Authorisation for school email accounts
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL.

10. Communication

Staff and Governors at Hillesley School use the email system set up by Focus Networks and provided by Office365 for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies: child protection and safeguarding, behaviour, anti-bullying, data protection and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use, the expectations, roles and responsibilities for staff around filtering and monitoring, online safeguarding issues including cyber-bullying and the risks of online radicalisation through Prevent awareness training.

All staff members will receive refresher online safety training including the expectations, roles and responsibilities for staff around filtering and monitoring at least once each academic year as part of safeguarding training, as well as relevant updates at other times, as required (for example through emails and staff meetings).

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. In addition, the DSL and Safeguarding Governor will undertake training on web filtering and monitoring of school systems as part of their lead responsibility for this.

Governors and Volunteers will receive training and updates for online safety, including the expectations, roles and responsibilities around filtering and monitoring and online safeguarding issues as applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

12. Filtering & Monitoring

All staff have a responsibility to monitor pupils whilst online and to report any potential areas of concern, including the potential for students to bypass systems, and any potential over-blocking. They can submit concerns at any point using the procedures detailed in our Child Protection and Safeguarding Policy, and will be asked for feedback at the time of the regular checks which will take place during staff meetings.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding training as well as via acceptable use agreements and regular training reminders in the light of the annual review and regular checks that will be carried out.

At Hillesley School:

- web filtering is provided by Focus Networks and EXA Networks on the school site
- changes can be made by Focus Networks and EXA Networks
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from Focus Networks

- regular checks are made half termly by Focus Networks to ensure filtering is still active and functioning everywhere and reported to the DSL
- an annual review is carried out as part of the online safety audit to ensure a whole school approach

At Hillesley School staff physically monitor children whilst they are online due to our small cohorts.

13. Monitoring arrangements

The school's approach to online safety is reviewed within the context of an annual Online Safety Risk Assessment and Audit, which is a collaborative effort led by the DSL.

This policy will be reviewed annually by the DSL/Headteacher/Safeguarding Governor. At every review, the policy will be shared and agreed by the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff Code of Conduct/Behaviour
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Remote Learning policy

Appendix 1: Acceptable use agreement for pupils and parents/carers

Acceptable use of the school's ICT facilities and internet: agreement for pupils

Name of pupil:

When I use the school's ICT systems (like computers or iPads) and get onto the internet in school or at home I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given and try my hardest to remember them
- Never share my password with anyone, including my friends
- Never open any attachments or click on links without asking my teacher first
- Never use chat rooms
- Never use the computers or IT equipment to break school rules
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

Pupil agreement: I understand that the school will check the websites I visit and monitor how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet, including using Google Classroom for remote learning.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's IT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I agree to:

- Always use the school's IT systems and internet responsibly, including the G Suite platform, and ensure that pupils in my care do so too.
- Undertake annual training on filtering and monitoring and cyber security in schools, including acting upon regular updates via emails and staff meetings.
- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- Supervise, guide and monitor children carefully when engaged in learning activities involving online technology (including extra-curricular, extended school activities, if relevant, and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Monitor SEND/vulnerable pupils on a 1:1 basis when using online technology
- Consider potential dangers and the age appropriateness of websites.
- Inform the designated safeguarding lead (DSL) if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material by following the school's reporting system as detailed in the Child Protection and Safeguarding Policy.
- Inform the DSL if I have any potential concerns regarding filtering and monitoring, and cyber security, regardless of how small.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with your responsibilities in terms of filtering and monitoring of online technology in school?	
Are you familiar with your responsibilities in terms of cyber security at school and at home if you are using work devices?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**