Hill View Primary School
The best in everyone™
Part of United Learning

Hill View Primary School Online Safety Policy

Updated September 2025

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. This policy details the procedures in place to support safe and responsible use of the internet by all members of the school community.

Date of last central office review:	SEPTEMBER 2021	Review Period:	Annually
Date of next central office review:	SEPTEMBER 2022	Owner:	Claire Ferens
Date of next school level review:	September 2026		
Type of policy:	United Learning Policy	Local Governing Body	Approves Policy

Contents

1. Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	04.11.2025
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator- Danielle Reid Senior Leadership Team
Monitoring will take place at regular intervals:	Once a year.
The Safeguarding Governor will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	At least once a year.
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	21/09/26
Should serious online safety incidents take place, the following external persons/agencies should be informed as necessary:	LA Safeguarding Officer, Academy Group Officials, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of ○ students/pupils ○ parents/carers ○ staff

2. Scope of the Policy

This policy applies to all members of the Hill View Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Hill View Primary School digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the Hill View Primary School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the Hill View Primary School but is linked to membership of the Hill View Primary School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for

template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Hill View Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This Online Safety Policy works in conjunction with other policies, including those for ICT, child protection and safeguarding. The school's Online Safety is co-ordinated by the Designated Members of Staff for Safeguarding, with support from the Headteacher and ICT Leader.

3. Aims

Our Hill View Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

4. 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
- 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.

5. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school/academy:

5.1 The Local Governing Body (LGB)

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

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

All governors will:

- Ensure that 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.

The governor who oversees online safety is our Safeguarding Governor and is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This will be carried out by the LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of Online Safety Governor and this role includes:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant LGB meeting}

5.2 The Executive Head, Head of School and Senior Leadership Team

- The Executive Head and Head of School are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Executive Head and Head of School have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Executive Head, Head of School and the Senior Leadership Team} should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and should refer to the safeguarding policy.
- The Executive Head, Head of School and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Executive Head, Head of School and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Online Safety concerns should be reported on CPOMS.

- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

5.3 The designated safeguarding lead

Details of the school's DSL/DDSLs are set out in Annex C of Keeping Children Safe in Education (DfE).

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged 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.
- 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

  This list is not intended to be exhaustive.

5.4 IT management

The ICT technician 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;
- 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 fortnightly 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 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;

This list is not intended to be exhaustive.

5.5 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 and ensuring that pupils follow the school's terms on acceptable use;
- Working with the DSLs to ensure that any online safety incidents are logged 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;

This list is not intended to be exhaustive.

5.6 Parents

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.

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
- Training and guidance – National Online Safety
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

5.7 Visitors and members of the community

Visitors and members of the community who access Hill View Primary School systems or programmes, or use the school's ICT systems or internet as part of the wider Hill View Primary School provision will be made aware of this policy (when relevant) and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a Community User AUA before being provided with access to Hill View Primary School systems.

5.8 Pupils

- are responsible for using the Hill View Primary School digital technology systems in accordance with the student/pupil acceptable use agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

6. Education/Training

6.1 Educating Pupils- Online Safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PHSE. This curriculum is based on the objectives in 'Education for a Connected World framework' which aligns with the National Curriculum. Individual objectives can be found in the Computing topic flyers and the RSHE curriculum overview.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

In EYFS, pupils will be taught to:

- Recognise they can say not to somebody who asks them to do something that makes them feel sad, whether in person or online.
- Recognise ways to communicate online using technology, being able to describe ways that some people can be unkind online and how this can make others feel.
- Identify ways to find and put information on the internet.
- Recognise and can give some simple examples of rules to keep them safe and healthy when using technology.
- Give examples of their personal information and describe the people they can trust and share this with.
- Know that the work they create belongs to them and name their work so that others know it belongs to them.

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

- Use technology safely and respectfully, keeping personal information private. This includes understanding what passwords are and why they are important.
- Identify rules to keep them safe when using technology at school and at home.
- 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.*

All schools -

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

6.2 Pupils using the internet.

Internet use by pupils is important:

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- All pupils read and must abide by the rules detailed in the school's "Class Online Safety Agreement" before using any school ICT resource. This will be relaunched at the beginning of each academic year.
- 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.
- The purpose of the 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 access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use by pupils will enhance learning:

- The school Internet access is planned expressly for pupils' use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that supports the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content:

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is part of every subject.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported, where appropriate, to the business manager or ICT leader, who will take the necessary action ie: report to the Portal.
- The School ensures that the use of Internet derived materials by staff and by pupils complies with copyright law.

6.3 Educating Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Hill View Primary School will therefore seek to provide information and awareness of internet safety to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications
- Giving parents access to National Online Safety

This policy will also be shared with parents.

If parents 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.

6.3 Educating the wider community.

The Hill View Primary School will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered (dependent of levels of staffing) through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Hill View Primary School website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

6.4 Educating and training staff/volunteers.

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal online safety training will be made available to staff via National Online Safety. All staff receive annual online safety training with is supplemented with updated throughout the year.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Hill View Primary School online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process. This online safety policy and its updates will be presented to and discussed by staff in staff meetings and training sessions.
- The Online Safety Lead (or other nominated person) will provide advice, guidance and training to individuals as required.

6.5 Educating and training staff/volunteers.

Members of the LGB should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

This may be offered in several ways:

- Attendance at training provided by the Local Authority/United Learning/National Governors Association/or other relevant organisation.
- Participation in Hill View Primary School training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

7. Protecting children from online abuse

Taken from the NSPCC "Protecting children from online abuse" (23.12.2020)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse • sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

7.1 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.)

7.2 Emotional Abuse

7.3 Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery);

This is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

7.4 Sexual abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish Government, 2014; Wales Safeguarding Procedures Project Board, 2019). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not,
- forcing or encouraging a child to take part in sexual activity,
- making a child take their clothes off or touch someone else's genitals,
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus.

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts,
- not taking proper measures to prevent a child being exposed to sexual activities by others,
- making a child masturbate while others watch,
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images,
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

7.5 Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2018; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2019).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.
Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity
- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be too scared to tell anyone what's happening because they don’t want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online,
- send or post sexually explicit images of themselves,
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

7.6 Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-toface by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However, extremists attempt to influence vulnerable people, the internet invariably plays some kind of role … being widely used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos and friend lists.

7.7 The school's response to online abuse

To help prevent online abuse 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 examples of online abuse with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on examples of online abuse 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 online abuse, 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.

A 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.

8. Mobile Technologies (including BYOD/BYOT)

At this time, mobile phones are not allowed to be used by students of parents on school site. If a child is in year 5 or 6, they may bring a mobile phone to school but it is at their own risk. It must be given to their teacher and locked away for the duration of the school day. At no point, do staff taken responsibility for a pupil's mobile phone.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

For information about staff using their own device, please refer to the school's the Bring Your Own Device (BYOD) policy.

9.1 Use of digital and video images

- Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked each September to notify the school, in writing, if they give permission for the school to use their child's photograph in school publications (which includes the school website).
- Images of staff are not published without consent from that member of staff.

For more information, refer to the school's use of digital and video images policy.

9.2 Email:

- Staff are advised to use their school email addresses for any school related correspondence but to be aware that this is not a secure system. Passwords should be considered for documents that contain sensitive information.
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- Social emailing interferes with learning and is restricted.

- The forwarding of chain letters is not permitted.

9.3 Published content and the school website:

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not be published.
- Email addresses are generally not published, to avoid spam harvesting. Contact forms are used where possible.
- The Headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

9.4 Social networking and personal publishing:

- Social networking sites and news groups are blocked unless a specific use is approved.
- Pupils are advised not to, and educated about the risks of, signing up to any social networking site that is not age appropriate. eg. Facebook
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline telephone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They are educated to consider how public the information is and when and how to use private areas. Advice is given regarding background detail in a photograph which could identify a pupil or his/her location eg: house number, street name, school or shopping centre.
- Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of any images.
- Pupils are advised and educated about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- The School is aware that bullying can take place through online activity, in particular social networking, especially when a space has been setup without a password and others are invited to see the bully's comments.
- See "Acceptable Use of ICT Policy" for further information relating to staff use of social networking.

10 Data Protection

When sharing information staff will ensure they comply with group data protection policies and keep records of disclosures as required by these policies.

11 Technical – infrastructure/equipment, filtering and monitoring

Hill View Primary School has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the Hill View Primary School online safety policy/acceptable use agreements. Hill View Primary School should also check their Local Authority/MAT /other relevant body policies on these technical issues.

Hill View Primary School will be responsible for ensuring that the Hill View Primary School infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Managing Internet access:

- The security of the school information systems will be reviewed regularly.
- The technical infrastructure is secure – support is provided by Turn-it-On.
- All users have clearly defined access rights to Hill View Primary School technical systems and devices.
- All users are provided with a username and secure password by Turn It On, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- Users are only able to access networks and devices by using a password.
- The "master/administrator" passwords for the Hill View Primary School systems, used by the Network Manager (or other person) must also be available to the Head/Principal or other nominated senior leader and kept in a secure place (e.g. Hill View Primary School's safe)
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Virus protection is installed and updated regularly.
- The school uses EXA broadband through Turn It On and Sophos Antivirus through Oxfordshire County Council.
- Portable media should not be used without specific permission and a virus check.
- Unapproved systems utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.
- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The Hill View Primary School has provided enhanced user-level filtering.
- Hill View Primary School's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- If there is a there is an actual/potential technical incident/security breach, the Turn It On are notified immediately.
- Supply teachers have access to a supply logon. Trainee teachers have access to their own email and logon.
- An acceptable use policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download executable files and installing programmes on school devices.

12 How the school will respond to issues of misuse

It is hoped that all members of the Hill View Primary School community will be responsible users of digital technologies, who understand and follow Hill View Primary School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour ○ the sending of obscene materials to a child ○ adult material which potentially breaches the Obscene Publications Act ○ criminally

racist material ○ promotion of terrorism or extremism ○ offences under the Computer Misuse Act ○ other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the Hill View Primary School and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Specific pupil/staff misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and as set out in the Pupil User Agreement. 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 ICT 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.

13 References, further reading and useful links

GOV.UK (30.6.2020), 'Guidance: Education for a Connected World', Available at: https://www.gov.uk/government/publications/education-for-a-connected-world

LGfL (2021), 'Online Safety and Safeguarding', Available at: https://www.lgfl.net/onlinesafety/default.aspx

National Online Safety (2021), 'Online Safety Education for the Whole School Community', Available at: https://nationalonlinesafety.com/

NSPCC Learning 23.12.2020), 'Protecting children from online abuse', Available at: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

SWGfL (2020), 'Hill View Primary School Online Safety Policy Template', Available at: https://swgfl.org.uk/assets/documents/online-safety-policy-templates-without-appendicies.pdf The Key (23.12.2020), 'Online safety policy: models and examples', Available at: https://schoolleaders.thekeysupport.com/policy-expert/pastoral/online-safety-policy-modelexamples/#section-0

United Learning (2021), 'Policies Portal', Available at: https://hub.unitedlearning.org.uk/sites/policies