

# Gorse Hill Primary School



## Internet Safety Policy

Review Policy	Annually
Updated	February 2018, October 2023
Ratified by Governors	March 2018
Responsible Person	Head Teacher

## **Introduction**

For clarity, the internet safety policy uses the following terms unless otherwise stated:

**Users** - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

**Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

**School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

**Wider school community** – students, all staff, governing body, parents (*insert others appropriate to your own school needs*).

## **Vision**

Safeguarding is a serious matter; at Gorse Hill Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as internet safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an internet safety incident, whichever is sooner.

## **Aims**

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

## **Policy Governance**

### **Governing Body**

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any internet safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure internet safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of internet safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.



### **Computing Coordinator**

Reporting to the governing body, the Head Teacher has overall responsibility for internet safety within our school. The day-to-day management of this will be delegated to a member of staff, the internet safety Officer, as indicated below.

The Head Teacher will ensure that:

- Internet safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated internet safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All internet safety incidents are dealt with promptly and appropriately.

### **Internet safety Officer**

The day-to-day duty of internet safety Officer is devolved to *the Computing Coordinator*.

The Internet Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head Teacher, governing body on all internet safety matters.
- Engage with parents and the school community on internet safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the internet safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical internet safety measures in school are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical internet safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher, Local Authority Technical Support and responsible governor to decide on what reports may be appropriate for viewing.



**Technical support staff** are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Operating System updates are regularly monitored and devices updated as appropriate.
  - Any internet safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the internet safety officer and Head Teacher.
  - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters
  - The IT System Administrator password is to be changed on a regular basis.

### **All Staff**

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any internet safety incident is reported to the internet safety Officer (and an internet safety Incident report is made), or in his/her absence to the Head Teacher. If you are unsure, the matter is to be raised with the internet safety Officer or the Head Teacher to make a decision.
- The reporting procedure contained within this internet safety policy are fully understood.

### **All Students**

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy (see Appendix 1 – student copy found in each student’s planner); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Internet safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

### **Parents and Carers**

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent leaflets, school newsletters and the school website, the school will keep parents up to date with new and emerging internet safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy, inside the school planner, before any access can be granted to school ICT equipment or services.

### **Buildings and Health and Safety Committee**

Internet Safety has been delegated to the Buildings & Health and Safety Committee is responsible:

- to advise on changes to the internet safety policy.
- to establish the effectiveness (or not) of internet safety training and awareness in the school.
- to recommend further initiatives for internet safety training and awareness at the school.

The Buildings and Health and Safety Committee meets on a termly basis.

## **Technology**

Gorse Hill Primary School uses a range of devices including PC's, laptops, Apple Macs, Tablets and other hand held devices. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

**Internet Filtering** – we use 'Bloxx' software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Local Authority, ICT Co-ordinator, internet safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.

**Email Filtering** – we use 'Sophos' software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

**Encryption** – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

**Passwords** – all staff and students will be unable to access any device without a username and password. Staff and student passwords will change if there has been a compromise. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

## **Smoothwall Software**

As an additional safety measure, the school has purchased Smoothwall software to run on all of its hardware in line with Keeping Children Safe in Education Sept 2023. Smoothwall Software filters use of the internet, it allows for staff to freeze computer screens and it produces usage reports and alerts the technicians and DSLs if there has been a security breach.

## **Safe Use**

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this internet safety and the staff Acceptable Use Policy; students/parents upon signing the acceptance of the Acceptable Use Policy within the school planner.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

**Photos and videos** – Digital media such as photos and videos are covered in the Photo/Media Parent Permission letter, and reiterated here for clarity (See Appendix 4). All parents must write to the school if

they do not wish their child to be photographed or videoed. Without a written letter of refusal to photograph, the school will assume parental permission has been granted.

**Social Networking** – there are many social networking services available; Gorse Hill Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Gorse Hill Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Internet Safety Officer who will advise the Head Teacher and request a decision to be made. Any new service will be risk assessed before use is permitted.

- Twitter – used by the school as a broadcast service (see Twitter Policy Appendix 2).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Parents’ refusal letters (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a licence which allows for such use (i.e. creative commons).

**Notice and take down policy** – should it come to the school’s attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working week.

**Incidents** - Any internet safety incident is to be brought to the immediate attention of the internet safety Officer, or in his/her absence the Head Teacher. The internet safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

**Training and Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Gorse Hill Primary School will have an annual programme of training which is suitable to the audience e.g. Internet safety week or Staff training.

Internet safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning. (See Appendix 1 internet safety Curriculum)

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The Internet Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD.

The internet safety Training Programme can be found at [www.thechildprotectioncompany.com](http://www.thechildprotectioncompany.com) and all staff and governor certificates of completing the programme are held on file by the DSL.

Gorse Hill Primary School – Internet Safety Policy – Updated October 2023



## Appendix 1:

### Acceptable Use of the Internet Policy for Staff.

The computer network and laptops are owned by the school, and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Acceptable Internet Use Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the school office for safeguarding purposes.

- All Internet activity should be appropriate to staff professional activity or the children's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Users are responsible for all email sent and for contacts made that may result in email being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

### Laptops

- Laptops are insured if they are accidentally or maliciously stolen by means of forced entry or assault whilst on school premises.
- If a laptop has been stolen the police need to be notified and a crime reference obtained.
- Staff needs to be vigilant about where they store their laptop in school.
- Only Staff should move Laptop Trolleys.
- Staff are responsible for transport and return of laptops from their trolleys.
- Laptops will not be covered whilst in transit or left unattended in a vehicle.
- School insurance will not apply where the laptop has been left unattended in a private household.
- Laptops must only be connected to the internet at home through a firewall.

I agree to follow the guidelines for computer and Internet use as outlined above and in the school's Acceptable Use of the Internet Policy.



Appendix 2:

# Gorse Hill Primary School



## Twitter Policy

<b>Review Policy</b>	<b>Annually</b>
<b>Adopted on</b>	<b>February 2018</b>
<b>Ratified by Governors</b>	<b>March 2018</b>
<b>Responsible Person</b>	<b>Head Teacher</b>

## **Rationale**

The rationale of this policy is to explain acceptable use of Twitter relating to Gorse Hill Primary School's twitter accounts (Currently @GorseHillPE).

This policy relates to staff, children, parents and governors. The policy will therefore aim to explain the purpose of Twitter in Gorse Hill Primary School and the benefits that will arise from its proper use.

It will also deal with any potential pitfalls from using this communication tool.

### **What is Twitter?**

Twitter is used primarily as a method of communication made up of 140 characters called a 'Tweet'. Tweets tend to reference people, places, and/or activities to which the said referee can respond. Tweeters either directly reference another person or broadcast information to which others can reply and respond. Twitter users are able to follow or be followed. To follow somebody / something ensures that all of their activity and comments appear in the followers news feed. The obvious benefit of having followers is that the information you broadcast is instantly distributed into their news feed. Users can also private message each other when they don't want conversations to appear.

Currently, Twitter is only used as part of the PE curriculum.

@GorseHillPE will not enter into private discussions with others.

@GorseHillPE will be a public account searchable through the Twitter website.

**What is the primary purpose of Gorse Hill Primary School's Twitter Accounts?** @GorseHillPE and future accounts will be used to showcase work and achievements of children at Gorse Hill Primary School. It will also be used to demonstrate safe and responsible use of social media and encourage the use of 21st Century technology.

@GorseHillPE and future accounts will not be used as tools to support parental communication such as snow days, training day closures etc.

### **Who controls content for Gorse Hill Primary School's Twitter Accounts?**

The uploading of content for @GorseHillPE and future accounts will be undertaken by the senior management team (SMT) and teachers at Gorse Hill Primary School. These tweets will be overseen by the safety officer (See eSafety Policy).

Teachers will be responsible for the uploading of content, secure storage of the device used to tweet and the posting of children's pictures only where consent has been obtained from parents (See Photo/Media Parent Permission Letter)

### **Posting Etiquette When tweets are made from the Gorse Hill Primary School's Twitter Accounts**

A hashtag will always be included. The use of hashtags allows tweets to be grouped with similar hashtags therefore allowing tweets to be grouped together. Hashtags will always start with the following structure: #GHP This denominates the tweet is originating from Gorse Hill Primary School. This hashtag will then encompass additional text which directly relates to the tweet.

The list below is a suggested list for hashtags (although additional hashtags can be added at a request from the safety officer:

# GHPSClazz1 # GHPSClazz2 #GHPSClazz3 #GHPSClazz4 #GHPSClazz5 #GHPSClazz6 #GHPSClazz7  
#GHPSClazz8 #GHPSClazz9 #GHPSClazz10 #GHPSClazz11 #GHPSClazz12 #GHPSClazz13 #GHPSClazz14  
#GHPFS #GHPSLKS2 #GHPUKS2 #GHPKS2 #GHPWholeSchool

All tweets will be of a positive nature.

*On no occasion shall text speak be used when tweeting e.g. gr8, +ive, lol etc.*

All tweets should be grammatically correct. If a tweet does contain grammatical errors it will be removed and the teacher who posted the tweet will be informed.

### **Posting Tweets When Off-Site**

To protect the children at Gorse Hill Primary School tweeting whilst off site is not allowed. Any tweets that celebrate success off site e.g. a football tournament should be made on the journey back to school or whilst back at school.

This will ensure that followers of @GorseHillPE and future accounts cannot place a child and the school at a specific off site location.

### **Hardware**

All tweets which include images will be made only from school devices. Staff will not use their own devices to take images for posting on Twitter.

### **Tweeting Times**

The school will only tweet between the hours of 8am and 6pm from Monday to Friday.

### **Naming of People when tweeting**

A child's name will never be displayed. The tweet should instead focus on the achievement e.g. Great use of our new school computers to edit our writing by Class 4.

### **Photograph Consent**

A list has been compiled of children who are not to have their photographs published on the Internet (including Twitter). At the start of every academic year staff will be given a list of children who are not to have their photographs published on the Internet (including Twitter). Additionally a list will be placed on the shared drive for reference by all staff members.

When tweeting from within the phase or across the whole school, staff should be aware of children who are not to have their photographs published on the Internet (including Twitter).

### **Who can follow @GorseHillPE and future accounts?**

When @GorseHillPE and future accounts receives a follower it will make informed decisions on a case-by-case basis as to accept or decline the follower.

These decisions will be based upon a number of factors:

- The name of the individual as read on their Twitter account and whether this name correlates to that of a parent on the SIMS database;
- is a member of the Gorse Hill Primary teaching staff;
- Is a school governor;
- is a known and proper person to the SLT or safety officer;
- The quality of the biography of each individual as read in the bio section of their Twitter account;
- The images on view in the potential followers Twitter account.

In the unlikely event that a parent, or other suitable follower is inadvertently rejected, the safety officer will hear each individual on a case-by-case basis. These hearings will usually involve the prospective follower making themselves known in person to the above named persons, with their Twitter details, and should take no more than a few minutes.

### **Who will @GorseHillPE and future accounts follow?**

In order to protect itself from inappropriate content being distributed into its news feed, @GorseHillPE and future accounts will not actively seek to follow any other users.

This is to ensure that the tweets displayed on @GorseHillPE and future accounts relate directly to education and the achievements of children at Gorse Hill Primary School.

**What is inappropriate content and referencing and how will it be dealt with?** @GorseHillPE and future accounts welcome any referencing, mentions, or interactions that show the school in a positive light only.

Therefore, Gorse Hill Primary School deems any of the following as inappropriate:

- Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school;
- Unsuitable images or content posted into its feed;
- Unsuitable images or content finding its way from another's account into the @GorseHillPE and future accounts' feed.
- Images or text that infringe upon copyright;
- Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school.

Any inappropriate content will be deleted and its users will be removed, blocked, and, depending on the nature of the comment, reported to Twitter. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.

### **Retweeting from time to time @GorseHillPE and future accounts**

The school will decide on a tweet by tweet basis as to whether or not to retweet information from its own Twitter accounts.

The retweeting of tweets from other organisations shall be undertaken by members of the SMT.

### **Administration Information**

This policy was created on 4<sup>th</sup> April 2017 by Mr J.Trier.

Gorse Hill Primary School – Internet Safety Policy – Updated October 2023

This Policy was reviewed in October 2023 by Mrs L Bates

This policy was presented and accepted by the Governing Body on 6/3/18

This staff revisited this policy on 30<sup>th</sup> October 2023

This policy will be reviewed in October 2025.

This policy will be subject to an earlier revision should Gorse Hill Primary School decide to allow children to use Twitter in school.

At the moment, Twitter, unlike Facebook, has no age restriction and so its use is determined by the individual.

### **Signatures**

Headteacher

Staff Member

Governor

## Appendix 4:

Dear Parent / Carer,

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website, or in school displays, including digital photo frames.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely,

Head Teacher

# Image Consent Form

Name of the child's parent/carer: .....

Name of child:.....

Year group: .....

**Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (one for each child) should be returned to school as soon as possible. (Please Circle your response)**

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?

Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3<sup>rd</sup> parties at special events e.g. School productions or extra-curricular events?

Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school?

Yes / No

4. May we use your child's image on our school's online publications e.g. website / blog / twitter?

Yes / No

5. May we record your child on video?

Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event?

Yes / No

**I have read and understand the conditions of use attached to this form.**

Parent/Carer's signature

..... Name

(PRINT):.....

..... Date:

.....

**Non-return of this form by Monday 27<sup>th</sup> November will result in the school assuming that you give your permission for all of the above.**  
**Conditions of Use**

1. This form is valid for from September 2023 until September 2025 (two academic years).
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3<sup>rd</sup> Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

**Notes on Use of Images by the Media**

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.