Glenthorne High School

Achievement for all

Online Safety Policy

2025-26

Contents

1. Aims

Our schools 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Context** - Being exposed to illegal, inappropriate, or harmful content, such as pornography fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism
- **Contact** - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** - personal online behaviour that increases the likelihood of, or causes harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi nudes and/or pornography), sharing other explicit images an online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: 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.

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

This policy complies with our funding agreement and articles of association.

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

The governor who overseas online safety is the safeguarding governor.

All governors will.

- Ensure that they have read and understood this policy

- Agree and adhere to the terms on acceptable use on the school's ICT systems and the Internet (appendix 2)
- Ensure the online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, when necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher and 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
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety instance are logged and dealt with appropriately in line with this policy
- Ensuring that all incidents of cyber bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and or external services if necessary
- Providing regular reports on online safety in school to the head teacher and all governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures such as filtering and monitoring systems which were reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorists and extremist material.
- Ensuring that the schools 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 schools ICT systems on a termly 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.

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 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 (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any instance of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify 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 (appendices 1)

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

- What are the issues? - Homepage - UK Safer Internet Centre
- Hot Topics - Childnet — Online safety for young people
- Parent resource sheet - Childnet — Online safety for young people

3.7 Visitors are 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).

4. Educating pupils about online safety

Pupils will be told about online safety as part of the curriculum.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 3,** pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

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

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want to be shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- Thats sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information in data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report or find support, if they have been affected by those behaviours
- How pupils can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

5. Educating parents about online safety

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

Online safety will also be covered during parents' evening.

The school will let parents know:

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

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

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 repetitive, intentional harming of 1 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 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/ form tutors will discuss cyber-bullying with their tutor groups.

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

All staff and governors 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 specific instant 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 report the incident and provide the relevant material to the police as soon as is reasonably practical, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (SLT/Head of Years), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider it a material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person and/or
- The pupil and/or the parent refuse to delete the material themselves

If a staff member **suspects** a device **may** contain, and it did, some image of a child (also known as a nude or semi-nude image), they will.

- **Not** view the image
- Confiscated the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings, working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings, working with children and young people

- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the schools 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 and 3). 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 the 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 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile phones into school but are not permitted to use them at any time during the school day. If mobile phones are seen, heard or known to be used then the phone and sim card will be confiscated until the end f the half term. Sixthform pupils are permitted to use mobile phones in the common room and photograpy pupils may use their mobile devices to capture images, but only when directed to do so by staff members.

Any breach of this will trigger disciplinary action in line with the school behaviour policy and will result in confiscation of their device.

9. Staff using work devices outside of 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 lowercase letters, numbers, and special characters (e.g., asterisk or currency symbol)
- Ensuring the 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 by always installing 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 ICT Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our polices on behaviour and ICT and internet 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 schools 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 disciplinary procedures/ staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of this 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 and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and Internet Acceptable Use policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the schools ICT systems (like computers) and get onto the Internet in school I will:** • Always use the schools ICT systems and the Internet responsibly and for educational purposes only • Only use them when a teacher is present or with the teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I finished working on it **I will not:** • Access any inappropriate websites, including social networking sites, chat rooms and gaming sites, unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails or follow any links in emails without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to, or post any material that is pornographic, offensive, obscene, or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision • Use or wear Smart Glasses on school premises. **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school without a teacher's permission • I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the schools ICT systems and Internet when appropriately supervised by a member of school staff. I agree to the conditions set out above the pupils using the schools 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 (Governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of Governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 • Take photographs of pupils without checking with teachers first • Check 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 will only use the schools ICT systems and access the internet in school or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will 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. I will let the designated safeguarding lead (DSL) and ICT manager know 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. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (governor/volunteer/visitor):	**Date:**

Appendix 3: Acceptable use agreement (staff)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
Name of staff member:

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

- Use ICT equipment for anything other than professional purposes.
- Share passwords or security details with anyone except the Network Manager or Headteacher.
- Ignore password security requirements (passwords must be changed every three months).
- Store confidential or personal data outside WLT SharePoint or WLT OneDrive.
- Attempt to bypass internet filtering or access blocked content.
- Connect unauthorised devices without permission.
- Use Smart Glasses under any circumstances.
- Breach copyright or intellectual property laws by copying, editing, or duplicating media without permission.
- Install or run unlicensed software or streaming services.
- Access pupil/parent data without secure login and two-factor authentication when remote.
- Retain school email accounts or LGfL credentials after leaving employment.

When using personal devices in school or outside school, I will not:

- Use personal devices to access work systems without ensuring firewall, antivirus, and system updates are in place.
- Use personal mobile phones for anything other than emergencies or essential school business, or in view of pupils or parents.
- Use personal hotspots instead of school Wi-Fi.
- Share Wi-Fi passwords or connection details with pupils or guests.
- Share my personal phone number unless absolutely necessary and safe.

E-Safety and Online Security – I will not:

- 'Friend' pupils, former pupils (unless colleagues), on personal social media.
- Create or use school social media accounts without Headteacher approval, or post images of pupils or staff.
- Send electronic communications on school systems that are unprofessional or unclear.
- Fail to report safeguarding concerns to the Designated Safeguarding Lead or data breaches to the Data Protection Officer.
- Ignore harassment or abuse via electronic communication—these must be reported to the Headteacher immediately.
- Prevent IT staff from enforcing GDPR compliance, including moving or deleting non-compliant data.
- Block Headteacher-authorised access to staff files for disciplinary investigations under Trust protocols.

The Use of AI – I will not:

- Use any AI software other than school-approved tools (currently MS365 Copilot and OtterAI).
- Enter personal or identifiable data (staff, pupil, school) into AI tools.
- Upload images of staff, pupils, or the school into AI systems.
- Use AI to create fake images, misleading information, or harmful content.
- Fail to verify AI outputs for accuracy and bias.
- Provide AI tools for pupils. If pupils use AI for homework, they must disclose its purpose and extent.
- Use AI in ways that infringe legal responsibilities, including data protection, safeguarding, and intellectual property laws.
- Use AI without evaluating outputs for pedagogical value.

Signed Staff:	**Date:**

Appendix 4: 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?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, 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 taking cyber-bullying?	
Are there any areas of inline safety in which you would like training/further training?	