Online Safety Policy

Great Walstead School

Last Revision Date	August 2023
This policy is reviewed by	Deputy Head / IT Manager
Group	Pastoral/Academic
ISI Reference	
Next Review Date	August 2024

Tick which category this document refers to:

ISI requirement to be made available	✓
ISI requirement to be on website	✓
Internal staff only	✓
Internal students only	
Internal staff and students	
Statutory requirement to have on website (non ISI)	

Contents

---

1. Aims

Our school aims to:

> Have robust processes in place to ensure the online safety of pupils, staff (including service contractors, After School Activities coaches, VMTs or leads), 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:

> **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, 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 and 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 for 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 [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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will 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 oversees online safety as part of Child Protection is Edwina Andersson

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 IT systems and the internet (appendix 1)

> Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

> Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Head

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy 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 head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Working with the head, IT 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 incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

> Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

> Liaising with other agencies and/or external services if necessary

> Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The IT manager

The IT manager is responsible for:

> Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are 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 terrorist and extremist material

> Ensuring that the school's IT 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 IT systems on a weekly basis

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

> Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> Reporting to the Deputy Head any incidents of cyber-bullying which will be 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 service contractors, After School Activities coaches, VMTs or leads), 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 IT systems and the internet (appendix 1 or 3), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)

> Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

> Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

> Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

> Notify a member of staff or the head of any concerns or queries regarding this policy

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

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

> What are the issues? – UK Safer Internet Centre

> Hot topics – Childnet International

> Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the IT and L4L curriculum:

It is also taken from the [guidance on relationships education, relationships and sex education (RSE) and health education](#).

All schools have to teach:

> [Relationships education and health education](#) in primary schools

> [Relationships and sex education and health education](#) in secondary schools

In **Pre-Prep**, pupils will be taught to:

> Use technology safely and respectfully, keeping personal information private

> Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in the **Prep School** 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 Year 6**, pupils will know:

> That people sometimes behave differently online, including by pretending to be someone they are not

> That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

> The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

> How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

> How information and data is shared and used online

> What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

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

In **Year 7 and Year 8**, 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

The safe use of social media and the internet will also be covered in other subjects where relevant including the Learning For Life (L4L) lessons.

Where 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

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

Online safety will also be covered during parents' evenings.

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 they will be asked to access.

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

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The IT teachers 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 10 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, 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

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. However, pupils should not be carrying around a device. If a pupil brings a device to school they must hand it into the school office immediately. Occasionally electronic devices will be allowed to be taken on residential trips or for long journeys. The member of staff taking the trip must make suitable plans as to when the children can use their devices and for what purpose. When on a school trip, the member of staff has the right to examine a device.

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

> Cause harm, and/or

> Disrupt teaching, and/or

> Break any of the school rules

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

> Delete the material, or

> Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or

> Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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

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

7. Acceptable use of the internet in school

All pupils, parents, staff (including service contractors, After School Activities coaches, VMTs or leads), agency staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 or 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 fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff (including service contractors, After School Activities coaches, VMTs or leads), 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 or 3.

8. Staff using work devices outside school

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

> Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

> Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

> Making sure the device locks if left inactive for a period of time

> Not sharing the device among family or friends

> 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 3.

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 IT Manager (Kelly Pugh)

8.1 Internet and Social Media for staff (including service contractors, After School Activities coaches, VMTs or leads), agency staff, volunteers and governors

- All internet access is logged, monitored and traceable.

- Individuals should be aware that all web access is subject to filtering and content control to minimise access to inappropriate sites.

- Individuals involved in intentionally viewing or circulating inappropriate material will be disciplined and if necessary the police will be informed. This material may include, but is not limited to, bad language, pornography, extremism, online gambling

and posting confidential information about pupils or staff. If something appears unintentionally, please inform the Head of Computing so appropriate action can be taken. All unintentional access is logged.

- Individuals must never upload images or videos of children on to any website – except the official Great Walstead site (which would be done by the member of staff in charge of the website) or on to Tapestry. This includes a member of staff's own personal website or social network page. Such action would result in immediate disciplinary procedure

- Individuals must not have students or former pupils (under 18 years old) as part of their social network group, such as Facebook, Twitter, Instagram etc, or contact them using Instant Messaging or other internet based forms of communication. Such contact could result in disciplinary procedures.

- Individuals are advised not to have parents of current pupils as part of their social network group.

9. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

10. 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:

  o Abusive, harassing, and misogynistic messages

  o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

  o 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 will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Deputy Head and Head of Computing. At every review, the policy will be shared with the governing board. This review is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. 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 notice

> Complaints procedure

> GWS Professional Code of Conduct Policy

Acceptable use of the school's IT systems and internet: agreement for staff, governors, volunteers

Name of staff member/governor/volunteer:
When using the school's IT 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   • Share confidential information about the school, its pupils or staff, or other members of the community   • Access, modify or share data I'm not authorised to access, modify or share   • Promote private businesses, unless that business is directly related to the school   • Access, or attempt to access AI (Artificial intelligence) platforms or sources.   • Access, or attempt to access personal emails/data
I will only use the school's IT 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 IT 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 IT 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 IT systems and internet responsibly and ensure that pupils in my care do so too.

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

Appendix 2: Year 3 to Year 8 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 school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a 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've 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
- Use any inappropriate language
- Create, link to or post any material that is 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

If I bring a personal mobile phone or other personal electronic device into school:

- I will take it straight to the office in the morning when I arrive and collect it at the end of the day.

I agree that the school will monitor the websites I visit, the words I type on any program will also be recorded 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 school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

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

Appendix 3 Acceptable use of personal devices/accessing the internet while onsite at Great Walstead School: agreement for Service Contractors, After School Coaches, VMTs and Guest speakers

Name of ASA/Contractor:
- 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)   - I will not use my device while in the care of pupils unless I have been authorised to do by a member of the Designated Safeguarding Lead (DSL) and signed a risk assessment.   - I will not access my camera/take photos of pupils/staff or the school, unless I have been authorised to do so by the DSL, and completed a risk assessment   - I must keep my device on me at all times, and not leave unattended.   - I will not allow a pupil to use my device.   - I will not install any unauthorised software, or connect unauthorised hardware or devices to the school IT network.   - I will not share confidential information about the school, its pupils or staff, or other members of the community

I will only use my personal mobile device/internet for the purposes of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit when connected to GW WiFi.

I will take all reasonable steps to ensure that my personal device is kept secure at all times, and not left unattended.

I will let the designated safeguarding lead (DSL) and IT 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.

Signed:	**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, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

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