Watford Grammar School for Girls

Online Safety Policy

This policy adopted by Board of Governors	September 2023
Next review date	March 2025
Updated	2 years
Committee Responsible	Curriculum

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, 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, guidance, and links to other policies

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

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

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 receive termly updates about online safety as part of the Governors' Report.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that 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, where 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 headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

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

3.4 The Assistant Head for IT

The Assistant Head for IT takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher, IT strategic lead and other staff, as necessary, to address any online safety issues or incidents
- Working with the DSL to ensure that all online safety issues and incidents are managed in line with the school child protection policy
- 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 incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.5 The IT strategic lead

The IT strategic lead 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents of which he is aware are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying of which he is aware are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use

- Ensuring that any online safety incidents of which they are aware are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying of which they are aware 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.

3.7 Parents

Parents are expected to:

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

3.8 Visitors and members of the community

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

3.9 Responsibilities in relation to Filtering and Monitoring

Department for Education standards in relation to Filtering and Monitoring require the clear allocation of responsibilities in relation to Filtering and Monitoring.

The Governing Body has overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. An assigned governor is responsible for working with relevant staff in school, and reporting the Governing Body, so that they can be assured that standards are being met.

The DSL has lead responsibility for safeguarding and online safety.

At WGGS, the DSL, Assistant Head for IT and the Strategic Lead for IT work together to ensure that filtering and monitoring is undertaken effectively.

- Day-to-day management of filtering and monitoring systems is overseen by the IT strategic lead and the IT team.
- Alerts from the filtering and monitoring systems are sent to the DSL, Assistant Head for IT and the Strategic Lead for IT. The DSL and Assistant Head ensure that these are actioned swiftly in line with normal safeguarding protocols.

The DSL, Assistant Head and Strategic Lead meet at least twice a year to undertake a formal review of filtering and monitoring. At the first meeting in each academic year, a full review of online safety in the school will also be undertaken. These meetings are attended by the assigned governor.

Additional meetings of this group will be convened as needed. Circumstances in which this might arise would be:

i) When new software or services are being procured.
ii) If a new way of working is being introduced.
iii) If a safeguarding risk linked to filtering and monitoring has been identified.

Outcomes of these meetings are shared with the full SLT, so that they have oversight of online safety measures.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The school's curriculum for doing this will be published on the website.

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 parent information evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the SLT lead for IT. 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 one person or group by another person or group, where the relationship involves an imbalance of power.

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.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information 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 Safeguarding and Anti-bullying policies.

6.3 Examining electronic devices

Whilst investigating incidents of behaviour, or supporting a student with a safeguarding concern, it is sometimes the case that a member of staff will find it helpful to see content on a student device. For example, it may be helpful for a member of staff to see screenshots linked to an issue of cyber-bullying.

In these circumstances, the following steps will be taken:

a) The member of staff will ask the student if they may see the content. If the student refuses, the member of staff will not compel the student, but will make a DSP aware and seek guidance.

b) If the student agrees, the member of staff will, before viewing the content, ask the student to describe what is on the screen. This is to avoid a member of staff inadvertently viewing youth produced sexual imagery.

c) If the member of staff is in any doubt about whether they should view the content or not, they should not view the content, but immediately contact a DSP for guidance.

d) If a member of staff views content on a student device, and judges that a copy needs to be retained in school for records, the member of staff will ask the student to take a screenshot using their device, and send this to the school email address of the member of staff. This content should then be transferred to CPOMS, and the email deleted from the staff email account.

There is guidance in the Behaviour Policy about the school's protocol for conducting searches. There is also guidance in the Safeguarding Policy about youth-produced sexual imagery, and reference should be made to these policies as needed.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to confirm their acceptance of an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors.

8. Pupils using mobile devices in school

Mobile phones are not permitted to be used on the school site. There are limited exceptions to this for sixth formers, who may use mobile phones in their social and work areas and, with teacher permission, in lessons for work-related activity.

If a pupil breaches the school policy on mobile phones, the phone will be confiscated and will be held by the Headteacher.

Students may bring a laptop or tablet into site, and use this with teacher permission during lesson time, and also during morning break. Full details of this are set out in the IT policy.

9. Staff using personal devices

Teaching staff are provided with school laptops, and non-teaching staff an appropriate desktop or laptop.. These should be the only devices used for work purposes in school. It should normally be the case that staff with laptops use these, rather than personal devices, if working off-site.

If a member of staff uses a personal device for work purposes off-site then they must use school-approved remote solutions.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will take action in accordance with the principles in our Behaviour Policy.

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

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

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 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.

12. Monitoring arrangements

Online safety issues will be logged on CPOMS, in line with normal safeguarding practice.

This policy will be reviewed every year by the Assistant Head with responsibility for IT. At every review, the policy will be shared with the governing board.

Appendix: Acceptable use policies

Acceptable Use Policy: Students

I understand that IT systems in school - including the internet, email, digital video and mobile technologies - are provided for educational purposes.

Learning effectively

- I will use the school IT systems to support my learning.
- I will listen carefully to the advice I am given by my teachers, and use IT as they show me in order to help me learn.

Keeping safe

- I will choose a strong password. I will not reveal it to anyone. I will only log on to the school network/learning platform with my own user name and password.
- If I discover an unsuitable site, I will switch the screen off and immediately tell a teacher.
- I will not bypass or attempt to bypass any of the security features provided at the school.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately
- If I feel bullied online then I will tell my parent/ carer or a teacher.
- For school-related activities, I will only use my school email address.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone via the internet.

Showing respect for others

- I will make sure that all digital communication with students, teachers or others is responsible, appropriate, inoffensive and sensible. This is both inside and outside of school, and includes use of social media.
- I will not use IT systems to bully or harass someone else.
- I will respect the privacy and ownership of others' work on-line at all times. I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will seek permission from my teacher before I take, store and distribute images, audio or videos of students and/ or staff. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do so from all media (i.e. USB, home computer etc)
- I will ensure that my digital activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring it into disrepute.

Taking care of our resources

- I will not download or install software on school technologies.
- I will log off when I have finished using a computer to allow others to use the machine.

- I will not deliberately damage computer, systems or networks and will report any incidents of damage I see to staff.
- I will not consume food or drink in the IT rooms.

My own device

I understand I may bring a device to school.

- I understand that I may use my own device for educational purposes only.
- I may use my device in lessons only if the teacher has given me permission.
- If I am using my device in class, I must keep my device in full view of the member of staff throughout the lesson.
- I understand that all incoming messages must be ignored completely until after a lesson. Audible alerts that a message has arrived must be turned off.
- I will not use my device to access text messages, personal emails, social media or other communications during lesson time.
- I must access the internet via the school wifi system. I may not connect to the internet via 3G, 4G or 5G.
- I am entirely responsible for the security and maintenance of any device and understand that school is under no obligation to investigate or compensate me or my parents for any loss or damage to devices whilst they are in school.
- I am responsible for charging my device and may not charge it during the day in school. The only exception to this is for sixth formers, who may charge devices in the Tennet Centre.
- I will not use my device at lunchtime. The only exceptions to this is if a member of staff has given permission and for sixth formers in the Tennet Centre.
- I understand that if I do not use my device in line with these rules, I may be told that I cannot bring it to school.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer or even the police may be contacted.

I understand the school has the right to monitor my use of the school network to ensure that this Acceptable Use Agreement is being followed.

Acceptable Use Policy: staff

By using school IT systems, I agree to do so in line with a number of school policies, including the Communication Policy, Staff Code of Conduct, Data Protection Policy and Safeguarding Policy.

I also agree to the following summary of acceptable use.

Communicating professionally

I will ensure that all electronic communication with students, parents, carers, staff and others is compatible with my professional role and in line with school policies.

I will use school-approved methods only (school email accounts or Teams) for online professional contact with parents, carers and students.

Supporting cyber-security

I will maintain a strong password on my school accounts, and not disclose this to others.

I will report any cyber-security concern (such as a potential phishing email) to the IT team immediately.

I will use school devices only when working on-site. If I have a school laptop, I shall normally use this when working off-site.

Safeguarding others

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

If taking a photograph or video of students, I will only do this with appropriate consent, and only with school equipment.

I will report any online safeguarding concern of which I become aware immediately to a member of the DSP team.

I will report any cyber-bullying concern of which I become aware immediately to a member of the DSP team.

If working with the personal data of others, I will do so in line with the Data Protection policy. I will contact a member of the Data Protection team if I have concerns, and immediately report any potential breach.

I understand that school IT equipment is provided for professional purposes. Whilst personal use is permitted, this must not take place when students are present, interfere with my ability to do my role, or prevent others using school equipment.

I understand that all school devices are monitored.

Acceptable Use Policy: Governors and Volunteers

By using school IT systems, I agree to do so in line with a number of school policies, including the Data Protection Policy and Safeguarding Policy.

I also agree to the following summary of acceptable use.

Communicating professionally

I will ensure that all electronic communication is compatible with my role and in line with school policies.

I will use my school email address when undertaking school business.

Supporting cyber-security

I will maintain a strong password on any school account to which I have access, and not disclose this to others.

I will report any cyber-security concern (such as a potential phishing email) to the IT team immediately.

Safeguarding others

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I will report any online safeguarding concern of which I become aware immediately to a member of the DSP team.

I will report any cyber-bullying concern of which I become aware immediately to a member of the DSP team.

If working with the personal data of others, I will do so in line with the Data Protection policy. I will contact a member of the Data Protection team if I have concerns, and immediately report any potential breach.

I understand that school email systems are monitored.