Online Safety and IT Security Policy

Wood Green Academy

Approved by: Governors	**Date:** 7th October 2024
Last reviewed : Sept 2024	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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.

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

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Calvin Hussey.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and t.he 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 (DSL)

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- 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's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

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 on school devices and school networks, which are reviewed and updated at least annually 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
- Conducting a full security check and monitoring the school's ICT systems on a monthly 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

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 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.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by using classcharts or a face to face concern.
- Following correct procedures if they need to bypass the filtering and monitoring systems for educational purposes , which in the first instance requires contacting the DSL and IT Manager, in order to review the risk and relevance of the need, as well as implementing any additional measures to ensure safeguarding standards are met (on a needs basis).
- 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 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'

3.6 Parents/carers

Parents/carers are expected to:

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

Parents/carers 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
- Parent resource sheet – Childnet

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 2).

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

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

All schools have to teach Relationships and sex education and health education.

In **KS3**, 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 **KS4** 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 shared further and not to share personal material that 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
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and 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 people 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.

As a school we may choose to adapt our teaching about safeguarding, including online safety, to those vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings and parent information evenings.

The school will let parents/carers 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 and who from the school (if anyone) their child will be interacting with online

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

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

6. 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. Form 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 through the Step Up for Life programme 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 11 for more detail).

The school also provides access to information on cyber-bullying to parents/carers via the Online Safety pages of the academy website (with update notifications being published to parents/carers via ClassCharts and academy social media channels).

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

The headteacher, and any member of staff authorised to do so by the headteacher 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, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL/ DDSL.
- 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 co-operation

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 Deputy Head (Behaviour and Attendance) , Headteacher and DSL 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 if the 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/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate 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 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

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 / Searches and Confiscation Policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Wood Green recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Wood Green will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by Wood Green.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 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, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2

8. Pupils using mobile devices in school

Year 12 and 13 students may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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
- 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 that 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 policies on behaviour and the WGA 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 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 Low level concern or Safeguarding Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that 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, threatening, 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

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the DSL and IT Manager. At every review, the policy will be shared with the governing board. The review (such as the one available here) 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:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Low Level concerns Policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT Acceptable Use Policy (staff / students)

Appendix 1: **ICT Acceptable Use Policy for Wood Green Academy** (Students/Parents/Carers)

I understand that I may face sanctions under the school's behaviour policy if I misuse any WGA ICT Systems as detailed in the ICT Acceptable Use Policy.
I have read, understood, and agreed to the Acceptable ICT Use Policy.
All students who use any Wood Green Academy ICT facilities, equipment, and online services, or who connect to the academy network are required to accept the following Acceptable Use Policy.
In accepting this policy, all users agree to the following:

1. **Inappropriate Content**
   - I will not view, store, or share inappropriate content on any academy device, network drive, or online storage provider. This includes (but is not limited to): 1.1 Files or messages containing unsuitable content or offensive language. 1.2 Files which violate copyright law, such as pirated videos, music, or software. 1.3 Files or messages that promote activities contrary to the ethos of Wood Green Academy (e.g., bullying, racism, terrorism). 1.4 Games, except those related to teaching and learning.

2. **Account Security**
   - I will ensure my password is unique to my school account and not easily guessable.
   - I will not share my login details with anyone and will keep them secret.
   - I will not change other users' passwords and will only edit or delete my own files. I will not view or change other users' files.

3. **Device Security**
   - I will not allow others to use devices loaned to me by the Academy. All activity on loan devices is logged and monitored.

4. **Responsible Internet Use**
   - I will use the internet responsibly and will not visit inappropriate websites.
   - I will not tamper with device settings or attempt to bypass security restrictions, including using proxy sites or VPNs.

5. **Communication**
   - I will not send, display, or print offensive or inappropriate content, including messages, images, sounds, or videos.
   - I will not use obscene, harassing, or threatening language in any form of communication.

6. **Respect for ICT Resources**
   - I will not damage ICT facilities or take equipment without permission.
   - I will only install authorised software and apps on academy devices.
   - I will not intentionally damage software or introduce viruses and will take preventive measures against them.
   - I will not waste resources, such as printing multiple copies of the same document.

7. **Network Access**
   - I will not attempt to log into the academy's network with a personal device.
   - I will not use others' login details to access devices, the network, or online services.

8. **Privacy and Respect**

- I will not use personal devices to record or store media of other WGA community members.
- I will not use academy devices to record or store media of other WGA community members unless directed by staff.
- I will not capture or distribute media from online sources that reference WGA community members without permission.

9. **Authorised Use of AI**
   - I will use AI technologies for educational purposes as directed by teachers and in accordance with age requirements of the AI platform used.
   - I will uphold academic integrity and properly cite AI-generated content, following teacher guidance.
   - I will avoid malpractice, including using AI to gain unauthorised access to information or manipulate data.
   - I will consider the ethical implications of using AI, respecting fairness, transparency, and accountability.
   - I will adhere to data privacy and security policies when using AI technologies.

10. **Reporting Concerns**
   - I will report anything that makes me feel uncomfortable or worried to a relevant member of staff or use the “Speak Out” button on the academy website.
   - If I receive inappropriate messages, images, or videos, I will not respond but will save and report them immediately.

11. **Personal Information and Online Safety**
   - I will not give out personal information without academy or parental permission.
   - I will not arrange to meet someone I only know online unless accompanied by a trusted adult.
   - I will respect age restrictions on websites and social networks.
   - I will not use school email or user details to sign up for social media or other online services.
   - I will use the school network and online services only for school-related work and as directed by staff.
   - I will not claim internet-sourced material as my own in my work.

I understand that if I fail to comply with this policy, I may be denied access to the computer network and/or other online services for a period determined by the Headteacher or senior staff. Further disciplinary action may be taken depending on the nature of the offence.

Appendix2: ICT Acceptable Use agreement for Wood Green Academy (staff, governors, volunteers and visitors)

All staff (teaching and non-teaching) at Wood Green Academy, as well as governors and visitors who use ICT facilities, equipment, and online services, or who connect to the academy network, are required to accept the following Acceptable Use Policy.

Wood Green Academy actively monitors all ICT use, including websites visited, internet searches, messages sent/received, apps and files viewed, created, or downloaded. This includes all websites accessed, including secure (HTTPS) websites, and any personal devices connected to the academy's network.

In accepting this policy, all users agree to the following:

1. Inappropriate Content

- I will not view, store, or share inappropriate content on any academy device, network drive, or online storage provider. This includes (but is not limited to):
    - Any files or messages containing unsuitable content or offensive language.
    - Any files which violate copyright law, such as downloaded/ripped content like videos, music, or software.
    - Any files or messages that promote any activity contrary to the ethos of Wood Green Academy (e.g., bullying, racism, terrorism).
    - Any games, with the exception of those related to teaching and learning.

2. Account Security

- I will not allow other users to use any of my login details and will keep my logins, IDs, and passwords secret. This includes colleagues, family members, and friends.

3. Device Security

- I will not allow anyone (other users, family members, friends, etc.) to use devices loaned to me by the Academy, as all activity is logged and monitored.
- I will ensure that my WGA electronic device(s) are logged out or "screen-locked" when left unattended.

4. Responsible Internet Use

- I will use the internet responsibly and will not visit websites that may contain materials considered inappropriate.
- I will not tamper with computer settings or attempt to bypass restrictions put in place for my safety, including the use of proxy sites or VPNs to access sites blocked by the academy.

5. Communication

- I will not send, display, or print offensive or inappropriate content, including messages, images, sounds, or videos.
- I will not use obscene, harassing, or threatening language in any form of communication (e.g., emails).

6. Respect for ICT Resources

- I will not damage ICT facilities or take ICT equipment from rooms without prior permission.
- I will only install software and apps on academy devices for which I have permission and only when the appropriate license is in place.
- I will not intentionally damage computer software (e.g., by knowingly introducing a virus) and will take preventive measures (e.g., not opening or downloading email attachments from unknown sources).
- I will not intentionally waste resources (e.g., printing multiple copies of the same document).

7. Personal Devices

- Staff must not use personal devices for the purpose of taking or storing photographic, audio, or video recordings of any other member of the WGA community (students, teaching staff, support staff). Exceptions may be granted, but only when authorised by a member of the Senior Leadership Team, IT Manager, or Head of eLearning.

8. Online and Social Media

- Staff must not capture (screen recordings, screenshots, audio capture, physical recordings), communicate, and/or distribute content that includes image, video, audio, or textual reference to other members of the Wood Green Academy community. Exceptions may be granted in line with the WGA Social Media Policy, when authorised by a member of the Senior Leadership Team, Network Manager, or Head of eLearning.

9. Privacy and Respect

- I will not use personal devices to record or store media of other WGA community members without their consent.
- I will not use academy devices to record or store media of other WGA community members unless directed by senior staff.
- I will not capture or distribute media from online sources that reference WGA community members without permission.

10. Reporting Concerns

- I will report anything that makes me feel uncomfortable or worried to a relevant member of senior staff.
- If I receive inappropriate messages, images, or videos, I will not respond but will save and report them immediately.

11. Personal Information and Online Safety

- I will not give out personal information without academy or parental permission.
- I will not use school email or user details to sign up for social media or other online services.
- I will not claim internet-sourced material as my own in my work.

12. Authorized Use of AI

- Staff members are permitted to use AI technologies (e.g., Microsoft CoPilot using WGA sign-in credentials) for educational and professional purposes in alignment with their roles and responsibilities within WGA. This can include, but is not limited to, the creation of resources, analysis of data, and support for the assessment of learner work. Any AI-generated content must be clearly cited as such for all users and audiences (including learners).

  Data Privacy and Security

- Staff should handle AI-generated data with the same level of care and confidentiality as other sensitive information. DO NOT enter personal details of staff or learners into AI. If using AI to support data analysis, personal identifying features must not be used.

Assessment

- When using AI to support the assessment of learner work, it cannot be used for summative assessment or for the provision of attainment grades or scores. AI can be used to generate formative feedback. Staff must conduct sample checking and make learners aware of the use of AI for the generation of any assessment, providing opportunities for learners to challenge and query the efficacy of the AI-generated feedback. Staff using AI for assessment must have undertaken relevant CPD before doing so.

Ethical Considerations

- Users must be aware of and adhere to ethical considerations when using AI technologies, ensuring that their actions respect human rights, diversity, and the well-being of individuals.

Transparency and Accountability

- When using AI systems with learners and colleagues, staff should strive to understand and communicate the capabilities and limitations of the technology.
- Users must be accountable for the outcomes of AI applications under their control, taking responsibility for any decisions or actions influenced by AI technologies.

Avoiding Discrimination and Bias

- Staff should be mindful of the potential biases inherent in AI algorithms and take steps to mitigate any discriminatory outcomes.
- Regularly review and assess AI systems to identify and address biases that may arise during usage.

Reporting Concerns

- Any concerns related to the ethical use, privacy, or security of AI technologies should be promptly reported to the relevant line manager or senior member of staff at WGA and the IT Helpdesk.

I understand that if I fail to comply with this policy, I may be denied access to the computer network and/or other online services for a period determined by the Headteacher or senior staff. Further disciplinary action may be taken depending on the nature of the offence.

Appendix 3: 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**