FOUNDATION FOR GROWTH
WOOTTON PARK ACADEMY TRUST
'Ipsum quod faciendum est diutius'

Title	Online Safety Policy ***Includes Acceptable Use Policy (AUP)***
Year	2025/ 2026
Author	Head of School/ Headteacher
Date approved by CEO on behalf of the Trust	March 2026
Review Date	March 2027

Contents

1. Aims....3
2. Legislation and guidance....3
3. Roles and responsibilities....3
4. Educating learners about online safety....6
5. Educating parents about online safety....7
6. Cyber-bullying....7
7. Acceptable use of the internet in school....9
8. Learners using mobile devices in school....9
9. Remote Education……..……9
10. Staff using work devices outside school....9
11. How the school will respond to issues of misuse....9
12. Training....10
13. Monitoring arrangements....10
14. Links with other policies....10
Appendix 1: Online Safety Group……...11
Appendix 2: ICT Acceptable Use Policy Agreement (AUP) for EYFS and KS1 (Learners & Parents/ Carers……13
Appendix 3: ICT Acceptable Use Policy Agreement (AUP) for KS2, KS3, KS4 and KS5 (Learners & Parents/ ……..14
Appendix 3: ICT Acceptable Use Policy Agreement (AUP) for staff, trustees, volunteers and visitors……15

1. Aims

Our school aims to:

- ✓Have robust processes in place to ensure the online safety of learners, staff, volunteers and trustees
- ✓Identify and support groups of learners 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.
- ✓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, anti-Semitism, radicalisation and extremism
- **Contact –** being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct –** personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce –** risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996, 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 learners' 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 Online Safety Group

It is everybody's responsibility to ensure that all learners are safe when accessing the resources online. In order to include all stakeholders, our Online Safety group includes members of staff and learners to ensure that all needs and duties are being met. See Appendix 1 for details of the Online Safety Group.

Alongside the Online Safety Group, some stakeholders also have additional responsibilities;

3.2 The Trustees

The Trustees have overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

The Trustees 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 Trustees 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 Trustees 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 Trustees should ensure learners are taught how to keep themselves and others safe, including keeping safe online.

The Trustees 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 Trustee who oversees online safety is the safeguarding trustee.

All Trustees 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 the internet (appendix 4)
- 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 learners 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

3.3 The Head of School/ Headteacher

The Head of School/ Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.4 The Designated Safeguarding Lead (DSL)

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

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

- Supporting the Head of School/ Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of School/ Headteacher and Trustees 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 lead to make sure the appropriate systems and processes are in place
- Working with the Head of School/ Headteacher, ICT lead 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 safeguarding and 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 schools to the CEO and/or Trustees

- 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.

3.5 The ICT Provider and ICT Lead

The ICT Provider and ICT Lead are 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 learners 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 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 (appendix 4), and ensuring that learners follow the school's terms on acceptable use (appendices 2 and 3)
- 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 informing the ICT Lead and DSL.
- Following the correct procedures by informing the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- 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'

This list is not intended to be exhaustive.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School/ Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 2 and 3)

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

There is also an online safety section for parents/carers on our school website and updates are sent home through our termly safeguarding newsletter.

3.8 Visitors and members of the community

Visitors and members of the community who use a 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 4).

4. Educating learners about online safety

Learners will be taught about online safety as part of the curriculum. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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

In **Key Stage 1**, learners 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.

Learners in **Key Stage 2** 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 Primary School**, learners 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;
- ✓ How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, learners 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.

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

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

By the **end of Secondary School**, they 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 which is sent to them;
- ✓ What to do and where to get support to report material or manage issues online;
- ✓ The impact of viewing harmful content;

- ✓ That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- ✓ That sharing and viewing indecent images of children (including those created by children) is a criminal offence which 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.

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

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

The school will use assemblies to raise learners' awareness of the dangers that can be encountered online. This will also be addressed through national agendas such as Safer Internet Day.

5. Educating parents/carers about online safety

The school will raise parents/carers awareness of internet safety in letters or other communications home. This policy will also be shared with parents/carers on our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School/ 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 learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners 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 learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their class/tutor groups, and the issue will be addressed in assemblies.

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, trustees and PCCAB members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learner, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers, via e-mail and through the termly Safeguarding Newsletter, so 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 trust will follow the processes set out in their school behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

- Poses a risk to staff or learners, 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 learners and staff. If the search is not urgent, they will seek advice from Head of School/ Headteacher.
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the learner'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 Head of School/ Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider 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 learner 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 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 learners 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 learners' 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, learners and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Wootton Park Academy Trust recognises that AI has many uses to help learners 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.

Wootton Park Academy Trust will treat any use of AI to bully learners in line with the 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 the trust. For more information in regards to AI at Wootton Park Academy Trust, please see our AI policy.

7. Acceptable use of the internet in school

All learners, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 2 to 4). 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 learners, staff, volunteers, trusteess 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 2 to 4.

8. Learners using mobile devices in school

Learners may bring mobile devices into school, but are not permitted to use them during the school day. Please refer to the **'Mobile Phone Policy'** for more information.

8.2 Learners in the VI form at Wotton Park School

Learners in VI form can bring devices on site and use these in the designated VI Form area for the purpose of research and study, but not outside this area, e.g. in corridors etc. This is to ensure we do not compromise the ethos and rules of the rest of the school. Phones should be switched off when moving around the building and attending lessons. VI Form Learners should sign the 'Bring Your Own Device Agreement' should they wish to use their devices in this way.

9. Remote Education

If learners are asked to work from home, it is important that sites we are asking them to use have been certified as safe by the teacher. Where possible, please provide a list of websites/ platforms for sites that can be used for research/ information.

If learners are accessing their education remotely for a longer period of time, the school will make regular contact with the learner and remind them of online safety expectations. For more information on Remote Education, please see our Remote Learning policy.

10. Staff using work devices outside of the school building

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 4.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice the ICT Lead.

11. How the school will respond to issues of misuse

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

12. 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 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 learners can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs 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.

Trustees and PCCAB members 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.

13. Monitoring arrangements

The DSL logs all safeguarding issues related to online safety. This information is held on My Concern.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the Trustees.

14. Links with other policies

This online safety policy is linked to our:

- ✓Child protection and safeguarding policy;
- ✓Behaviour policy;
- ✓Staff disciplinary procedures;
- ✓Data protection policy and privacy notices;
- ✓Complaints procedure;
- ✓AI policy;
- ✓Remote Learning policy

Appendix 1

Wootton Park Academy Trust

Online Safety Group

Members

- Online Safety Lead
- Designated Safeguarding Lead
- ICT Lead
- Computing Curriculum Leader/ Subject Leader
- Safeguarding Trustee
- Online Safety Ambassadors (Learners)

Aims

• To draw upon the wide and varied knowledge of others with different skillsets, experience and opinions.
• To consider and plan for new statutory requirements such as Keeping Children Safe in Education; ensuring that any new needs are met.
• To ensure there is a broad and balanced online safety curriculum, considering the needs and vulnerabilities according to age and other factors such as SEND, advances in technology etc.
• To monitor the impact of this curriculum, identify any gaps or weak areas.
• To plan for annual initiatives such as Anti-Bullying Week or Safer Internet Day.
• To spread the workload, building resilience within the school.
• To monitor and review policy.
• To monitor incidents and ensure that they have been dealt with in accordance with school policy.
• To risk-assess any new technology in the school prior to purchase.
• To engage the school community - working together to benefit all.

Responsibilities

Whole Group

• To discuss new or developing issues, e.g. new apps children/young people are using, new games, emerging risks etc.
• To review the online safety policy annually or in response to an incident.
• To monitor online safety incident log (note: not suitable for learners to be present)
• To discuss training needs, including staff, parent/community awareness.
• To raise new community initiatives in response to training needs or as a result of polls/surveys.
• To coordinate annual events such as Anti-Bullying Week or Safer Internet Day

Trustee Link

• To independently review minutes to ensure that accurate records are kept.

Online Safety Leads

- To oversee the trust's online safety strategies development and implementation
- To ensure that minutes taken and actions are delegated and actioned.
- To advise on the correct use and implementation of filtering categories to ensure age-related filtering is appropriate to education.

DSL/ IT Lead

• To ensure that training, education, initiatives, incidents etc. are in line with trust policy and individual school's strategic plan.
• To brief SLT on meeting minutes and any actions and/or concerns.

DSL Lead

• Liaise with other agencies for any county-wide/national areas of concern.
• Retain responsibility for the online safety incident log (if you have one) alongside other safeguarding/child protection logs and ensure safeguarding incidents pertaining to online safety have been actioned accordingly.

IT Lead

• To ensure that the group is kept fully updated with any network security incidents or areas of concern.
• To advise on the correct use and implementation of filtering categories to ensure age-related filtering is appropriate to education.
• To advise on other ICT aspects, e.g. monitoring requirements in line with Keeping Children Safe in Education.

Curriculum Leads/ Subject Leads

• To review the online safety curriculum with other relevant members of staff, e.g. PSHE lead, ensuring that it is tailored to fit the needs of all students and statutory requirements.
• Keep up to date with new risks, issues, developments and resources in the area of online safety and brief the group accordingly.

Learner Ambassadors

Learners should be at the forefront of the group and any initiatives. It is important the school understands their concerns and their ideas as to how these concerns can be tackled. Opinions of learners should be a primary focus; they can bring useful insights and experience to the group through meetings/polls/questionnaires with other learners. To develop and implement actions from the online safety council meetings.

Appendix 2 *(Taken from Wootton Park Academy Trust Online Safety Policy)*

EYFS and KS1 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of Learner:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
If using Artificial Intelligence for school work, I will;
• I can use AI to learn, but I must do your own work.
• never type my name, address, or other private information into AI tools.
• Only use AI for good things.
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (learner):	**Date:**
Parent/carer 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3*(Taken from Wootton Park Academy Trust's Online Safety Policy)*

KS2, KS3 and KS4 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	
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 that 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 • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will ensure that it is locked in the QuietCase pouch whilst on the school premises. **If using Artificial Intelligence for school work, I will;** • only use it as a learning tool and not as a replacement for original work. • not enter in any personal data for myself or anybody else who could be identified. • **not use AI** to create or share inappropriate, misleading, or harmful content, including deepfakes, false information, or offensive material. Any misuse will result in disciplinary action per school policies. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (learner):	**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 4 *(Taken from Wootton Park Academy Trust's Online Safety Policy)*

Acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that 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 **If I bring a personal mobile phone or other personal electronic device into school:** • I will ensure that I only use it in the designated areas. • I understand if I use my mobile phone in any other areas of the school, sanctions will apply. **If using Artificial Intelligence for school work, I will;** • Review any AI-generated content used for lessons or communication for accuracy, bias, and appropriateness before sharing with learners or parents. • not input sensitive or identifiable learner information (e.g., names, grades, behavioral records) into AI systems to comply with data protection laws • not use AI to generate as a substitute for teacher knowledge.	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**