Warrington Primary Academy Trust

Online Safety Policy

Ratified: 15 July 2024

Next Review Date: July 2025

Policy Responsibilities and Review

Policy type:	Trust Wide Policy
Guidance:	KCSIE
Related policies:	Child Protection & Safeguarding Behaviour Staff Disciplinary Procedures Staff Code of Conduct Data Protection & Privacy Notices Complaints Procedure ICT & Internet Acceptable Use
Review frequency:	Annually
Committee responsible:	Quality of Education Committee
Chair signature:	
Changes in latest version:	New policy

Contents

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, governors and trustees
- 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

This policy is to safeguard the pupils of WPAT. There are 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
- 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 Local Governing Committee (LGC)

The Trust has overall responsibility for this policy and delegates the monitoring of this to LGCs, including holding the Headteacher to account for its implementation.

The LGC 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 LGC will also ensure 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 LGC will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training.

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

The LGC 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.

On each LGC there is a Governor who oversees online safety.

All Governors will:

- Ensure they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the Trusts ICT systems and the internet (appendix 3);
- 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 and 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 approach 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 DSL are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Headteacher, LGC and Trust 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 WPAT ICT Support Service (EDAC) to make sure the appropriate systems and processes are in place;
- Working with the Headteacher, WPAT ICT Support Services and other staff, as necessary, to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with the school child protection policy;
- Ensuring that any online safety incidents are logged on CPOMS 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 the LGC;
- Undertaking annual risk assessments that consider and reflect the risks children face;
- Ensuring 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 WPAT ICT Support Service

WPAT ICT Support Service 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; and
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors, 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;
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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

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 International
- Parent resource sheet – Childnet International

3.7 Visitors & 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the computing curriculum, though elements will be referred to within other subjects, particularly Personal Development. Each school has a system e.g. Project Evolve which is derived from the Education for a Connected World document.

All schools have to teach:

- Relationships education and health education in primary schools.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private; and
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour; and
- Identify a range of ways to report concerns about content and contact.

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

- That people sometimes behave differently online, including by pretending to be someone they are not;
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online;
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context); and

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

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 pupils with SEND.

5. Educating parents/carers about online safety

Each school will raise parent/carer awareness of internet safety in letters or other communications home, and in information via our website or social media page. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use; and
- 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 DSL.

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

6. 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 a victim.

Each 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. Teachers will discuss cyber-bullying with their class.

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

All staff, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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

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

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 or DSL;
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it; and
- Seek the pupil's cooperation.

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

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

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

If inappropriate material is found on the device, it is up to the 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; and
- 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;
- The schools behaviour 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.

The Trust 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.

The school will treat any use of AI to bully pupils 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 school.

7. Acceptable use of the internet in school

All pupils and parents/carers must sign the acceptable use agreement which is located in the children's planners at the start of every school year (appendix 1 and 2). Staff are asked to sign the code of conduct which includes the acceptable use agreement. Every visitor to the school must sign in on the Inventory system to acknowledge acceptable use of internet in school and understanding of safeguarding procedures.

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.

Each school monitors 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.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

For the children who choose to bring their mobile devices into school, it is expected that they are given to the class teacher for safe keeping until the end of the school day. Any mobile devices brought into school will remain the responsibility of the child.

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

9. 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. 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 code of conduct and disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - 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 will undertake child protection and safeguarding training, which will include online safety, annually. They will also update their knowledge and skills on the subject of online safety at regular intervals, at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

11. Monitoring Arrangements

All online safety concerns raised by staff are recorded on CPOMS and monitored by the DSL.

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

The Trusts Web Filtering Service is provided as part of the Network Service using a 3rd party supplier, Forcepoint. When this service was procured Warrington Borough Council (WBC) considered the statutory guidance and believe the solution provides 'appropriate web

filtering'. The technology uses a category system to define what type of content each website represents, such as education, business, drugs, malware etc. That category determines whether a school can or cannot access that specific site. Forcepoint have an Advanced Classification Engine that performs in depth, real-time inspection of content to categorise web sites and protect users from accessing inappropriate content and malware. Each school has categories deemed potentially harmful and/or inappropriate blocked by default and then can have rules to block or allow certain sites as per their individual requirements. The service, transparent to the end user, intercepts internet traffic from across the WPAT network and is designed to protect staff and learners as much as possible.

The WBCs ICT team look after the web filtering for WPAT and will investigate any web filtering related issues, including:

- Access to website containing inappropriate or potentially harmful material;
- Access to websites containing educational or related material deemed appropriate for your school; and
- Providing web access reports on an annual basis.

The ICT team (EDAC) also ensure that the service is maintained and is accessible for schools to use.

Appendix 1: Whole School Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE POLICY AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:
Signed by pupil: **Date:**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to may safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- If I arrange to meet people that I have only communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) unless I have permission of a member of staff to do so.
- I will act as I expect other to act toward me.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.
- I will only use my personal hand held/external devices (mobile phone/ USB devices etc) in school if I have permission I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risk and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Appendix 2: Parent/Carer Acceptable Use Policy Agreement

PARENT CARER ACCEPTABLE USE POLICY AGREEEMENT

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-Safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return expect the students/pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carer's Name:

Pupil Name:

Appendix 3: Acceptable Use Agreement (governors, 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 (unless for school purposes, e.g. Facebook • 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 to log in to the school's network using someone else's details • Take photographs of children 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
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 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 Leads (DSL) and Data Protection Officer 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 (governor/volunteer/visitor): **Date:**