UNIVERSITY OF WINCHESTER ACADEMY TRUST

ONLINE SAFETY AND SMARTPHONE POLICY

Approved by	LAC
Reviewed on	April 26
Next Review Date	April 27
Responsible person	CEO
Committee Responsible	LAC
Regularity of Review	Annual

1	**AIMS** The University of Winchester Academy Trust (UWINAT) 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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	**LEGLISATION & 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 › Meeting digital and technology standards › Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff › Relationships and sex education RSE and health 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	**SCOPE & DEFINITIONS** This policy applies to all members of the UWINAT community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school. For the avoidance of doubt: • Smartphone: internet-enabled mobile device capable of apps, browsing, camera, etc. • Brick phone: call/text only device with no internet access. • Personal electronic device: any privately owned digital device brought onto school premises. This policy applies during; clubs, extended provision, trips, including travel time.
4	**ROLES & RESPONSIBILITIES** **Local Academy Committee (LAC)** 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 and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online. The governing board will make sure that 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's 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 the school's safeguarding needs **Headteacher/Head of School**

- The headteacher and senior leadership team are responsible for ensuring:
- The Online Safety and Smartphone Policy is implemented and compliance with the policy is monitored.
- Staff receive suitable training and development to carry out their online safety roles.
- Robust reporting channels for online safety or smartphone use concerns and incidents exist (the school currently uses CPOMS and CEOP reporting tool)
- Online safety and smartphone use issues are embedded in all relevant school policies and procedures.

Designated Safeguarding Leads

- Leading day-to-day online safety and smartphone issues and establishing and reviewing the school's online safety and smartphone policies and procedures.
- ·Ensuring online safety is recognised across all safeguarding and child protection work.
- Coordinating participation in local and national online safety initiatives – including keeping up-to-date training from NCA (National Crime Agency) with CEOP Ambassador, annual training and use of Smartphones for children.
- Ensuring that online safety including smartphone free training for staff is integrated, current, and relevant.

All Staff

All staff have a duty of care to ensure the safety of children and to report any concerns about online safety, including use of Smartphones to the HEAD or a member of the DSL team.

Staff are responsible for:

- Consistently enforcing this policy within the school.
- Ensuring they model expected behaviours including only using mobile phones in adult only spaces such as the staff room or school offices.
- Modelling positive online behaviours and promoting a culture of online safety and smartphone usage.
- Embedding online safety in their teaching and school activities.
- Monitoring children's online activity, including smartphone use and reporting any concerns.
- Maintaining an awareness of current online safety issues and guidance.

Children

Children are responsible for:

- Engaging in age-appropriate online safety education, including the use of Smart Technology
- Knowing and adhering to school rules and policies regarding the use of digital technologies.
- Respecting the feelings and rights of others both online and offline.

	› Seeking help from trusted adults if they are concerned about something they have seen or experienced online **Parents and Carers** › Parents and carers have an essential role in ensuring their children use digital technologies safely and responsibly both in and out of school. Parents and carers are responsible for: › Modelling positive online behaviours and promoting a culture of online safety and smartphone use at home. › Discussing online safety with their children and reinforcing the school's approach and expectations. › Keeping up to date with online safety issues and the school's Online Safety and Smartphone Policy. › Informing the school of any online safety or smartphone concerns that may impact their child or other children at the school.
5	**ACCEPTABLE USE** › All members of the school community must adhere to the following acceptable use guidelines: › Use school devices for educational purposes only › Personal devices connected to the school network (for example governors requiring access for meetings) must be used in accordance with this policy › Do not access, share, or create inappropriate content or engage in any form of online bullying. › Report any online safety concerns to a trusted adult immediately **Use of Work Devices Out of School** › School-owned devices may only be used outside of school for educational purposes as directed by school staff. › Staff must ensure that sensitive information is stored securely, and devices are returned to school in good condition. › Children must not take school devices home without prior permission and must adhere to the school's acceptable use policy at all times.
6	**ONLINE SAFETY AND THE CURRICULUM** Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects: · Relationships and health education · PSHE · Computing Further details are available on the school curriculum coverage and content pages for the these subjects.

Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

· How to evaluate what they see online

·How to recognise techniques used for persuasion

· Acceptable and unacceptable online behaviour

· How to identify online risks

· How and when to seek support

· Knowledge and behaviours that are covered in the government's online media literacy strategy

Relevant members of staff, e.g. the SENCO and designated teacher for Looked After Children (LAC), will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

7	**SMARTPHONE-FREE SCHOOL FOR PUPILS** › Pupils may not bring smartphones to school unless express permission under medical grounds has been granted by the Headteacher/Head of School (see appendices for the relevant form). › If necessary, for Years 5 and 6 only, a 'brick phone' allowing voice calls and texts without internet access is allowed which must be handed in to the school office upon arrival (see appendices for suggestions of suitable phones). The expectation is that only a small number of pupils who walk to and from school unaccompanied may need to bring a phone to school. › Other internet-linked devices or devices that can take images or record (e.g., smartwatches) are not permitted › University of Winchester Academy trust schools promote a smartphone-free environment to encourage face-to-face interaction and reduce distractions (this is during the time any child is on the school premises, school trips and residentials). › **Parents/carers are encouraged to support this policy by ensuring that children do not bring smartphones to school.** › In the event of a child having a smart phone in school, it will be reported to the Headteacher/Head of School and reasonable steps will be made to address concerns and risks › Reasonable adjustments will be considered on a case-by-case basis for pupils with SEND or medical needs, in line with the Equality Act 2010. **Risks Associated with Smartphone Use** › Smartphones offer advanced features, including internet access and social media, which can lead to various risks: › Cyberbullying: Smartphones can facilitate harassment, making it difficult for pupils to escape bullying. › Exposure to inappropriate content: Unfiltered internet access can expose children to unsuitable material. › Mental Health Concerns: Excessive use can contribute to anxiety and depression. › Distraction from Learning: Smartphones can disrupt the learning process. › Privacy and Security Risks: Children may not understand how to protect their personal information, leading to exploitation. › Self-obsession and Personal Curation: The culture of selfies and social media can create confidence issues. **Artificial Intelligence (AI)** Generative 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 Gemini. The University of Winchester Academy Trust recognises that AI has many uses 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. UWINAT schools will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policy.

	Any use of artificial intelligence by staff should be carried out in accordance with our AI usage policy.
8	**CONFISCATION AND SANCTIONS** › Our schools reserve the right to use sanctions for breaches of the mobile phone policy, including confiscation and suspension. DfE guidance on searching & confiscation will be followed. › Any smartphone or internet-linked device found on school premises will be confiscated and returned only to a parent or carer. › Brick phones are permitted for the journey to and from school for Years 5 & 6, but if they are not handed in to the class teacher during school hours, they will also be confiscated and returned to a parent or carer. › If a child's phone has been confiscated for any of the reasons above, a parent or carer will be called by the school to collect their child and phone at the end of the day. › Repeated violations may result in consequences in line with our Behaviour Policy. › Staff are protected from liability when confiscating items if they act lawfully and proportionately.
9	**ENCOURAGEMENT OF ALTERNATIVES** › If parents wish to track their child when walking to and from school, this should be done using a separate device outside school hours only, as tracking devices are not permitted on school premises or trips. We have provided a list of alternative phone options which allow for location monitoring and GPS. › Where children are due to attend school trips or off-site visits, we do not allow the use of any tracking or GPS device for an individual child. This causes increased risk to all children involved and is against our safeguarding and child protection policy.
10	**CRITICAL INCIDENT MANAGEMENT** **In the event of an online safety incident, the school will:** › Follow established procedures for reporting, recording, and responding to incidents. › Ensure that all staff are trained to manage online safety incidents effectively. › Provide support and guidance for those affected by online safety incidents. › Review and adapt policies and procedures following any critical incident to improve future responses.
11	**MONITORING AND REVIEW** UWINAT will regularly monitor and evaluate the implementation and effectiveness of this Online Safety Policy, including: › Annual review of the policy and associated procedures. › Monitoring of online safety incidents and concerns. › Gathering feedback from the school community on the policy and its implementation. › Keeping up-to-date with the latest online safety guidance and best practices.

12	**COMMUNICATING THE POLICY** › The policy will be communicated to all members of the school community, including pupils and parents, to ensure clarity and consistency in its implementation. › Regular reminders will be provided to pupils about the policy and its rationale
13	**REPORTING CONCERNS** › If any pupil, staff member, or family has concerns regarding internet or mobile phone use, they should report it to the school's Headteacher/Head of School. All concerns will be treated seriously and addressed in line with the school's safeguarding and behavioural policies.
14	The University of Winchester Academy Trust is committed to ensuring the online safety of all members of its community. This policy, along with our safeguarding policy, provides a comprehensive framework to guide our schools' approach, ensuring that all stakeholders understand their roles and responsibilities in maintaining a safe online environment. It also addresses the potential dangers of smartphones while promoting responsible habits among pupils. We invite parents to collaborate with us in creating a culture of safety and respect within our school communities.

Appendix 1:
Alternative Options to Smart Phones

This list is not comprehensive and will be updated annually based on the changes in technology and the available device son the market. As a school we have focussed the options firstly associated with keeping children safe and allowing a level of independence for our children in Year 5 and 6. Children in classes below Year 5 and not permitted to have any electronic communication device in school.

Nokia 105 £19.99
Sim-free mobile phone
Talk, text and wireless FM radio
Amazing battery life
Torch and snake game

Nokia 2660 Flip £50-60
Texts and phone calls
Very long lasting battery
Range of colours
Bright, colourful display (non pixelated text)
Built in FM radio, MP3 player and torch
Snake (and Tetris but you need to pay for the full game)
Single rear facing camera (no selfies!)

Nokia 5710 £74.99

Like an iPod with in-built wireless earbuds which charge when not in use
Inbuilt mp3 player with storage for thousands of songs
Inbuilt speaker Wireless FM radio Great sound quality Great battery life No wifi or whatsapp

Pinwheel £239 for the Samsung Plus 4 model or £479 Google Pixel 8A model. Plus £13.99 monthly for the Pinwheel Caregiver Portal

Modern, reliable kid phones with built-in parent management Device is designed to grow with your child, to meet their experience and maturity level.
You can create a contact safelist, monitor texts and calls and set schedules for when contacts and apps are available.
No web browser or social media apps, but hundreds of other vetted apps available, which you can choose to add when your child is ready, including banking, Google Maps, Spotify and Citymapper.
Inbuilt GPS locator

Sim cards

IMPORTANT – When you get a SIM card for your child's phone, make sure that it has NO DATA roaming, only calls and texts so that there **is no chance that they can access the internet.**

Appendix 2: Personal Electronic Devices Agreement Form

Parent personal electronic devices agreement

I, _____, recognise that the school bears no responsibility for personal electronic devices lost, damaged or stolen on school property or on journeys to and from school. I agree to the terms of this policy and will discuss the responsibility of owning a personal electronic device with my child (name) _____. I understand that a teacher may confiscate devices used in an unacceptable manner as detailed in the policy.

I have express agreement from the headteacher for my child to bring a personal device to school and agree to drop this into the school office at the start of each school day.

Signed by

Parent		**Date**	
Head teacher		**Date**	

I, _____, understand that bringing a personal electronic device to school is a privilege that may be taken away if I abuse it. I agree to abide by the policy and understand the consequences if I fail to do so.

Signed by

Pupil		**Date**	
Parent		**Date**	
Head teacher		**Date**	

UNIVERSITY OF
WINCHESTER
ACADEMY TRUST

Registered office:
Halterworth Primary School
Halterworth Lane
Romsey
Hampshire
SO519AD
Tel: 01794 512028
E: enquiries@uwinat.co.uk
W: www.uwinat.co.uk