Windmill Primary School

Online Safety Policy

Title	Online Safety Policy
Policy Owner	Mark Gibbons
Version	2026
Approved Date	July 2026
Approving Body	School Standards Committee (governors)
Next Review Date	July 2027

Version Control

Version	Last Modified	Last Modified By	Document Changes
2025	2025	Mark Gibbons	New policy
2026	2026	Mark Gibbons	Removed reference to Twitter

COMMUNITY ACADEMIES TRUST

The purposes of this policy:

At Windmill Primary School, we understand the responsibility we have as role models to educate our pupils on online safety issues, teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We are aware of the risks that our pupils face in relation to these technologies and ensure that they are taught how to react in a variety of situations to minimise risk to themselves or others. Windmill Primary School has a whole school approach to the safe use of digital technology and creating this safe learning environment includes three main elements: - a robust provision of network and internet security (provided by Telford and Wrekin Council) - policies and procedures with clear roles and responsibilities and a comprehensive online safety programme for pupils, staff and parents.

Roles and Responsibilities:

Online safety is the responsibility of all staff at Windmill Primary School and includes staff who do not use a computer or digital device as they must have an understanding of online safety and its importance.

The online safety curriculum is the responsibility of the computing coordinator (see computing policy) and has been shared and verified with Designated Safeguard Leads (DSL) and senior management. The online safety policy is to be written by and updated by the computing coordinator and checked with DSL and senior management. Staff need to be made aware of any changes to the policy. Staff are reminded/updated about online safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and must follow school online safety procedures. All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on school blogs or school social media sites.

- procedures in the event of misuse of technology by any member of the school community.
- their role in providing online safety education for pupils in line with the online safety long-term plan provided by the computing coordinator.

Managing the school online safety messages:

- promoting online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The online safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- Online safety posters will be displayed in all classrooms around the school.
- Internet Safety Week to be promoted every year.

Curriculum:

At Windmill Primary, we ensure that online safety is taught to pupils on a termly basis from Reception to Year 6. We have developed a long-term plan for online safety, which is accessible, and progressive, ensuring messages are reinforced each year in an engaging manner and are appropriate for each year group. Each term, every class must be taught two online safety lessons in addition to informal discussions and reminders whenever digital technology is being used. We are continually looking for new ways to promote online safety.

- We provide opportunities within a range of curriculum areas to teach about online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise, and formally as part of the curriculum.
- Pupils are aware of the impact of online bullying through online safety lessons and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Managing Internet Access:

- The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material,

which makes it both an invaluable resource for education as well as a potential risk to young people.

- Pupils will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to senior management. The unsuitable site must be reported to the internet provider (Telford and Wrekin Council) so it can be blocked. An incident like this should also be logged in the school's safeguarding and behaviour system (CPOMS).
- Pupils should only use messaging software if the teacher has allowed it and it is for educational purposes in a safe environment.
- Videos should be screened first by staff before being shown to pupils in lessons. • Pupils can search for videos and images for educational purposes, but this must be done in a controlled environment.
- Internet filtering is managed by our internet and network provider, Telford and Wrekin Council.
- Anti-virus management is controlled and monitored by our internet and network provider, Telford and Wrekin Council.

Security and Data Protection:

The school and all staff members comply with the Data Protection Act 2018.

- Personal data will be recorded, processed, transferred and made available according to the act.
- Password security is essential for staff, particularly as they are able to access and use pupil data.
- Staff have secure passwords, which are not shared with anyone.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.
- All staff computers must be locked when the member of staff is away from the machine.

- Staff devices, that have access to school email or the network, must have password, retina or fingerprint protection to ensure sensitive data is safe if the device is lost or misplaced.
- Staff must take care when opening email attachments and be aware of fake emails and scams. Protection against this is in place from our network and internet provider, Telford and Wrekin Council.
- Staff should use the 'freeze' or 'blank' option on interactive boards when viewing sensitive information e.g., school register

Cybercrime:

Cybercrime is a criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include.

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;
- Denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- Making, supplying, or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

If a member of staff suspects a member of the school community is involved in cybercrime, they will report it to the Designated Safeguarding Lead (or a deputy) who will deal with the incident – the Designated Safeguarding Lead (or a deputy) may need to seek further advice from agencies such as the police or Family Connect. In addition to this, if there are concerns about a child in this area, the Designated Safeguarding Lead (or a deputy), will consider referring the child into the 'Cyber Choices' programme National Crime Agency

Online safety Complaints/Incidents:

As a school, we take all precautions to always ensure online safety. However, due to the international scale and linked nature of internet content, the availability of mobile

technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for the material accessed or any consequences of this. Complaints should be made to the Headteacher through the appropriate channels. Incidents relating to online safety could involve staff, volunteers, visitors or pupils and in some cases may take place beyond school. Incidents may be in relation to unsuitable use or unsuitable material, or in extreme cases, illegal use or material. In either case, it is the responsibility of the staff member who witnessed the incident to follow it up in line with the school's behaviour policy. This may require them to inform a Designated Safeguard Lead or deal with the incident themselves, depending on the seriousness of what happened. In any case, it must be logged in our behaviour and safeguarding software (CPOMS). Any safeguarding issues, related to online safety, must be reported to Designated Safeguard Lead and logged in our behaviour and safeguarding software (CPOMS). When an incident has occurred and been passed on to a Designated Safeguarding Lead or member of the SLT, it is then their responsibility to take appropriate action.

Keeping Pupils Safe in Education states that:
The breadth of issues classified within online safety is considerable and ever-evolving, but can be categorised into four areas of risk:

1) **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
2) **contact:** being subjected to harmful online interaction with other users; for example: 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.
3) **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, 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
4) **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org).

Social Media:

At Windmill Primary School, we use social media (Facebook, Instagram and YouTube) and Class Dojo to promote pupils' achievements and work and to strengthen the link between home and school. Pupils' photos and work will only be posted on school social media sites and Class Dojo if permission is granted from parents or carers. Permission is given or denied by the child's parent or carer when they are admitted to the school. If this decision is changed, it is the parent or carers' responsibility to contact the school. Names of pupils should not be posted alongside the photo in any public domain.

Social media, staff:

Staff are advised to ensure that their personal social media accounts are private and to use their social media accounts responsibly. Staff can access these accounts in their free time during the workday but must only do this in designated areas of the school such as the staff room, out of view of the pupils.

Staff will:

- Ensure that their device can be locked (passcode/fingerprint or other means).
- Ensure that their device is kept out of reach of pupils.
- Ensure that their screensaver or wallpaper is suitable.

Staff should not make calls or send messages from their phones in any area of the school where they can be heard by the pupils. If a member of staff needs to make a call or send a message, it should be done in a designated area where no pupils are present (for example, the staffroom/staff office).

Online safety Outside of School:

Pupils have access to many forms of digital technology outside of school. The safe use of these technologies outside of school is the ultimate responsibility of the child's parents or carer(s). However, at Windmill, our whole school approach to online safety extends to all our families. We do and will give any information or advice to parents and carers that is requested regarding online safety. Pupils are encouraged to report incidents that happen outside of school to members of staff so that advice can be given and so action can be taken when appropriate.

Communication Devices:

Windmill Primary School is filled with a variety of communication technologies. These technologies have huge educational benefits, and we embrace the use of them. However, we also understand the importance that these technologies are only used by the appropriate people in school, at the appropriate times. We strongly discourage pupils from bringing mobile devices into school for a variety of reasons:

- Safeguarding the child and other pupils,
- They are expensive and we have very limited space to store them securely (we do recognise that older pupils may need to start bringing their own mobile phone, particularly in preparation for the transition to secondary school)
- Pupils must not use their phone for any purpose once on school grounds and they will switch it off at the school gate.
- Mobile phones must be dropped off in the main office where they can safely be stored away and picked up and the end of the school day (after the bell has rung)
- If a child does not follow the above rules, their phone will be confiscated, and their parent or guardian will be called.
- In these instances, the phone will be kept in school until a parent or guardian collects it.
- If any of these rules are broken repeatedly, the school has the right to ban any child from bringing their phone.
- If a child's phone gets damaged in any way, or lost on school grounds, it is not the school's responsibility.

Online-Bullying:

At Windmill we take online bullying very seriously. All incidents will be logged on CPOMS and SLT/DSLs will be made aware. An incident of online bullying will be dealt with in accordance with the procedures in the school's Behaviour Policy.

Films and TV programmes:

The viewing of Films and TV programmes in school will occur at various times throughout the year. We allow pupils to watch films either to further enhance the curriculum or as a

reward. Pupils in year Reception up to Year 4 will only be shown films rated U by the British Board of Film Classification (BBFC) unless parental consent is given for a PG film to be shown. Pupils in Year 5 and Year 6 will be shown films rated U and PG unless our families do not give permission for their child to be shown a PG film. To determine this, our families will sign consent at the beginning of their school life, and this is updated every new academic year. Should this information change then the child will no longer be allowed to view PG Films or TV programmes

Review:

Mark Gibbons
Updated July 2026
Review July 2027