The Windmills Junior School

E-Safety & Acceptable Use Policy – For pupils and staff

March 2025

Next Review: March 2026

(Full review every three years or when new information is published)

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The safeguarding governor will monitor the schools policies and effectiveness of ensuring online safety for children as part of their ongoing monitoring role – they will include this in their reports to the full governing board.

All governors will:

- Ensure that 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 3)

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

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, ICT technicians, school business manager and computing lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOms (schools recording system for all causes of concern 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
- Taking lead responsibility for understanding the filtering and monitoring systems and processes in place.

3.4 The ICT technician (JSPC – the school buys in technical support)

The ICT technician – overseen by the schools business manager - is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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

This list is not intended to be exhaustive and will change as the nature of ICT changes and when needed.

3.6 Parents

Parents 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 (appendices 1 and 2)

Parents 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 factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum: National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

This new requirement includes aspects about online safety.

Pupils 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**, 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*
- *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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, parent mail or on our virtual learning platform. This policy will also be shared with parents via the website.

Online safety will also be covered during assemblies, workshops and if applicable parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and then escalated up to a DSL.

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

6. Cyber-bullying

6.1 Definition –

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends 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.

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

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils, in year 5&6, may bring mobile devices into school, but are not permitted to use them during the day. They must hand them into their teacher at the beginning of the day and collect them at the end of the day.

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

Details from the behaviour policy:

Use of mobile phones: The school strongly discourages parents from providing their children with mobile phones throughout the primary phase due to increasing evidence about the damage that this does for their mental health and well-being, what they can access and how young people interact online. There is no reason why children in the lower school should need to have a phone at all and we do not allow children in these year groups to bring phones to school.

Mobile phones and watches are not to be used during the school day.

Mobile phones MUST be handed into the class teacher on arrival in the classroom. These will be stored in the teacher's cupboard (which is not always locked) during the day and returned at home time. The school takes no responsibility for lost or damaged phones and parents are agreeing to this by allowing their child to bring devices into school. They are not covered by the school's insurance policy.

Smart watches must NOT have access the internet or this MUST be turned off during the school using parental controls. These devices should only be used for telling the time. If smart watches are a distraction for children they will be removed from the child and stored in the same way that mobile phones are stored and returned at the end of the day.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted in line with GDPR guidance.

If staff have any concerns over the security of their device, they must seek advice from the SBM/ ICT technician.

Work devices must be used solely for work activities.

Where individuals are using their own computers to check emails and work they must not open and save any documents with pupil data on. They should use Office 365 and work 'in the cloud' to ensure that no data is inadvertently saved to the computer.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the HR staff disciplinary procedures and refer back to the 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.

11. Training

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

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

The 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.

Governors will receive information on how staff have been trained and our duty to keep children safe online.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

All staff, including DSLs, logs behaviour and safeguarding issues related to all causes of concern including online safety.

This policy will be reviewed every 2 years. At every review, the policy will be shared with the governing board.

13. 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
- ICT and internet acceptable use policy

Appendix 1: KS2 acceptable use agreement (pupils and parents/carers)

The Windmills Junior School recognises its duty for safeguarding and promoting the welfare of all children and as such has created this policy to protect children and ensure that they know how to use computers safely. We share this policy with all parents when their children start at our school so that they can talk through the expectations with their child. We ask the parent to acknowledge that they have discussed this with their child, and the child has agreed to the rules below. We collect this permission electronically.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

All learners must follow the rules in this policy when using school computers. Teachers will show learners how to use the computers appropriately and safely.

Learners who do not follow these rules may find:

- They are not allowed to use the computers,
- They can only use the computers if they are more closely watched.

When I use the school's ICT systems (like computers and iPads) 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 username 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 which might upset, distress or harm me or others
- always log off or shut down a computer when I'm finished working on it
- tell my teacher if I think someone has learned my password
- make sure that I use the equipment sensibly and take great care when carrying iPads and laptops to the trollies – putting them away safely and remembering to put them on charge

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
- 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
- tell my username and passwords to anyone else but my parents
- use other people's usernames and passwords or computers left logged in by them
- create or sending on the Internet any messages that might upset other people

If I bring a personal mobile phone or other personal electronic device into school (yr 5&6 only):

- I will hand it into my teacher in the morning on silent
- I know that if my phone is lost, stolen or damaged whilst on school property that this is not the responsibility of the school and they will not pay for a replacement

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

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. I have agreed to this on the MCAS App.

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people (teachers and supported by TAs). Applicable to role: YES/NO

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will avoid using the systems for personal use.
- I will not use personal social media apps/sites on school devices (e.g. face book / twitter).
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will ensure that my password is one that is not easily guessed and therefore secure. This must be made up of letters, numbers and symbols.
- I understand that I should not write down or store a password where it is possible that someone may access it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too and are taught about online safety.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission (checking the permission list for pupils).
- I will not use my personal equipment to record images, unless I have permission to do so.
- Where images are published (e.g. newsletters /on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities or reputation or impact on the reputation of the school.
- I will not use personal email addresses to correspond on school matters.

Using devices in school

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not 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 not try (unless I have permission) to make large downloads or uploads that might take up network capacity and prevent other users from being able to carry out their work.
- I will regularly rationalise items that I have uploaded, especially photographs and videos, keeping only those of good quality that will be used again
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission is gained from the Headteacher to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

Data Protection

- I will only transport, hold, disclose or share personal information about myself or others, as appropriate and in accordance with GDPR guidelines. Where digital personal data is transferred outside the secure local network, it must be password protected.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

Agreement

I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I understand that how I use ICT systems can potentially cause a data breach or a safeguarding issue and I accept these responsibilities and will work within the guidelines and policies agreed by the school.

Signed (staff member/governor/volunteer/visitor):	**Date:**