Online Safety Policy

The Willows Primary School

Explore - Dream - Discover

Contents

Contents

1. Aims

The Willows Primary School 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as child-to-child 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.

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
- Cyber-bullying: advice for headteachers and school staff
- Relationships and sex 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. Roles and responsibilities

a. The governing board

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, 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 coordinate meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety captures as provided by the designated safeguarding lead (DSL).

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

The governing board 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 those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is John Perry, our safeguarding link officer.

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
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some 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 or contextualised approach may often be more suitable

b. The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

c. The designated safeguarding lead

Details of the school's DSL, DSO and deputy DSLs 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:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- working with the governing board to review this policy and ensure the procedures and implementation are updated and reviewed regularly
- taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- working with the ICT manager to make sure the appropriate systems and processes are in place
- working with other staff, as necessary, to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the school's child protection policy
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- updating and delivering staff training on online safety
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the governing board
- undertaking annual risk assessments that consider and reflect the risks children face
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

In the event that the DSL was not available the deputy DSL would take the lead responsibility for the points above. They will have in the same training as the DSL and participate in regular safeguarding reviews to ensure they are able to fulfill their responsibilities.

d. The ICT management team

The ICT management team, provided via an external agency called Securus is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 regular basis.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Ensuring that any online safety incidents are reported to the DSL, logged and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are reported to school leaders and dealt with appropriately in line with the school's (Relational) Behaviour Policy.

e. 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, and ensuring that pupils follow the school's terms on acceptable use
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

f. 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

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 resource sheet – Childnet International

Parents will be sent regular newsletters during the school year to learn more about online safety both in school and at home.

g. 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. **All** schools have to teach Relationships education and health education in primary schools. Furthermore, pupils are taught about online safety as part of the computing curriculum.

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

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

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
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- 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 about online safety

The school will raise parents' awareness of internet safety through letters and in information via our website. This policy is also available on each school website.

The school will let parents know:

- what systems the school uses to filter and monitor online use
- 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 have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL.

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

6. Cyber-bullying

a. 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's (Relational) Behaviour Policy.)

b. 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. 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 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's Anti Bullying 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 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.

c. Examining electronic devices

The headteacher, and any member of SLT, can carry out a search of and confiscate any electronic device that they have identified through the monitoring and filtering procedure that;

- poses a risk to staff or pupils,
- and/or is evidence in relation to an offence.

Headteachers and staff they authorise have a statutory power to search a pupil or their possessions where they have reasonable grounds to suspect that the pupil may have a prohibited item that the member of staff reasonably suspects has been, or is likely to be used to commit an offence (Searching, Screening and Confiscation - GOV.UK).

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.
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- 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.

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/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 refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of 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

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

d. 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 Willows Primary School 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.

We will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed. Teaching staff are not permitted to use AI for teaching and learning purposes without expressed permission from the headteacher. Should a decision be made to use it, then staff members should carry out a risk assessment where new AI tools are being used.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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 and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils that walk to and from school on their own, with parental permission, are allowed to bring mobile devices into the school. These must be handed in to the class teacher at the start of the day and collected 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.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure.
This includes, but is not limited to:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- making sure the device locks if left inactive for a period of time
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- not sharing the device among family or friends
- keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school technician or the Evolve helpdesk.

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 acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and 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 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, 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, DSO and deputy DSL's 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 training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by consideration of risks, and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Contribution of Learners

The Willows acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- appointment of e-cadets
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection Policy
- (Relational) Behaviour Policy
- Anti-Bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints Procedure
- Staff and Volunteer AUA
- Pupil On-line Safety Agreement

Child Protection

The welfare of our children is paramount. To ensure the safety of our children, we adopt the following procedures:

- All regular volunteers must have been cleared by the Disclosure Barring Service (DBS). A certificate is issued to the individual to produce in school.
- In the unlikely event that a volunteer begins work before a DBS certificate is issued the school will obtain a check on the volunteer using the DBS children's barred list.
- All volunteers read the Volunteer Policy and sign a Volunteer Agreement.
- The Headteacher of the school will carry out a risk assessment to determine whether volunteers that do not attend regularly require a DBS check.
- All volunteers work under the supervision of the class teacher of the class to which they are assigned. Teachers retain responsibility for all children at all times, including the children's behaviour and the activity they are undertaking.
- Volunteers are never left alone with children and do not accompany children to the toilet.
- Volunteers do not accompany pupils on public transport unsupervised by a member of the school team.

Confidentiality

Volunteers in the school are bound by a code of confidentiality. Any concerns that volunteers have about the children they work with and/or come into contact with should be voiced with the class teacher and not with the parents of the child/persons outside school. Comments regarding children's behaviour or learning can be highly sensitive, and if taken out of context, can cause distress to the parents of a child if they hear about such issues through a third party rather than directly from the school. Volunteers who are concerned about anything another adult in the school does or says should raise the matter with the Headteacher.

Health and Safety

The school has a Health & Safety Policy and this is made available on request to volunteers working in the school. Class teachers ensure that volunteers are clear about emergency procedures (e.g. fire alarm evacuation) and about any safety aspects associated with a particular task (e.g. using DT equipment / accompanying children on visits). Volunteers need to exercise due care and attention and report any obvious hazards or concerns to the class teacher or a member of the leadership team.

Complaints Procedure

Any complaints made about a volunteer will be referred to the headteacher for investigation. Any complaints made by a volunteer will also be referred to the headteacher. The headteacher reserves the right to take the following action:

- to speak with a volunteer about a breach of the volunteer agreement
- offer an alternative placement for a volunteer
- inform the volunteer that the placement has been terminated.

The full Complaints Procedure is set out on the school website