NETHERFIELD
PRIMARY SCHOOL

**E-Safety Policy**

Date of last review: Autumn 2026
Date of next review: Autumn 2027

## Purpose

We help children use technology safely, confidently and respectfully. This policy applies to online learning and communication in school and at home. We act on concerns affecting a pupil's safety wherever the incident took place, including in games, messages and group chats outside school hours.

## Risks children may encounter

Content

Children may see upsetting, sexual, violent, discriminatory or extremist material. False or deliberately misleading information, including AI-generated images, can influence what children believe.

Contact

Adults or children may impersonate others, groom, exploit or put pressure on a child. A chatbot can simulate a trusted person and give harmful advice.

Conduct

Children can experience or cause harm through bullying, harassment, sharing private information or circulating intimate images, including images created using AI.

Commerce

Advertising, in-game spending, gambling-like features, phishing and financial scams can put children and their families at risk.

## How to raise a concern

A pupil can tell any trusted adult at school. Parents and carers can contact the school office and ask to speak to the designated safeguarding lead (DSL) or a deputy. Staff listen, take the child seriously, explain what will happen next and reassure them that abuse is never their fault.

Staff act immediately on a safeguarding concern, inform the DSL or a deputy and record the concern, decisions and action in line with the child protection policy. If a child is in immediate danger, call 999. If the DSL and deputies are unavailable, staff follow the child protection referral procedure without delay.

Where a nude or semi-nude image of a child is reported, staff refer it immediately to the DSL. They do not ask a pupil to show or send the image, or copy, save or forward it. The DSL assesses the risk, arranges support for the children involved and decides on contact with families and relevant agencies.

## How we keep children safe

### Filtering and monitoring

We filter access to harmful material on school devices and networks and use Securly to monitor activity. Filtering restricts access. Monitoring helps staff identify activity that may need a safeguarding response. Staff supervise pupils and report harmful material that gets through, or filtering that prevents legitimate learning.

The senior leader responsible for filtering and monitoring maintains the arrangements for routine reports and immediate high-risk alerts, including who receives them and who provides cover. The DSL assesses safeguarding alerts and records action. IT support investigates technical faults and checks that changes work.

Governors and trustees oversee the effectiveness of these arrangements. At least once each academic year, the responsible senior leader reviews them with the DSL and IT support. The review includes recorded checks of filtering on all internet-connected devices in relevant locations, including school devices used at home where applicable. We consider pupils' ages, additional needs and local safeguarding risks when reviewing provision.

### Staff and device use

All staff receive online safety training at induction, including their filtering, monitoring and reporting responsibilities. Training is refreshed regularly and safeguarding updates are provided at least annually. Staff and pupils follow the acceptable use policy. We protect personal data and report suspected breaches, malware or compromised accounts through the school's data protection and IT procedures.

Pupils do not access personal mobile phones during the school day, including breaks and lunchtime, except where an individual exception has been agreed under the mobile phone policy. Staff follow the school's restrictions on personal devices and use school-owned devices when working with or photographing children.

### Working with families

We explain to parents and carers how school devices are filtered and monitored, how to report a concern and how to reinforce online safety at home. For remote learning, we identify the sites pupils should use and who from school will communicate with them.

Related policies and guidance

Read alongside the school's child protection, behaviour, anti-bullying, acceptable use, mobile phone, data protection and RSHE policies.

Keeping children safe in education 2026, Part one and Part two

DfE filtering and monitoring core standard

DfE statutory RSHE guidance in force from September 2026

**What we teach children so that they are safer outside school:**

Computing, Relationships Education and Health Education develop these skills together. We revisit reporting in every year group. Teachers adapt examples and ways of asking for help to pupils' ages and communication needs, including using pictures, signs or a familiar adult.

| **Year 1** |
| --- |
| Identify personal information such as a name, address, school or password. Practise keeping a password private, asking before sharing a photograph and telling a trusted adult when something on screen feels upsetting or confusing. |
| **Year 2** |
| Use kind words online and recognise that messages can affect someone's feelings. Identify trusted adults at home and school. Practise what to say about worrying content or contact, including when somebody asks for secrecy. Keep asking until someone helps. |
| **Year 3** |
| Recognise online bullying, including in games and group chats, and explain how it can affect wellbeing. Practise reporting it for yourself or a friend without passing hurtful messages on. Explain why games and apps have age ratings and when to leave a chat or get adult help. |
| **Year 4** |
| Distinguish fact, opinion and misleading claims. Compare search results and explore how filters, advertising and the selection of information affect what appears. Choose a username that protects personal details. Recognise that someone can pretend to be a child. Check permission before reusing images, music or video. |
| **Year 5** |
| Recognise scams, phishing, pressure to spend in games and the risks of sharing personal details or location. Practise declining requests for information or pictures, respecting another person's refusal, and blocking or reporting contact with adult help. Explain how gaming can become hard to stop and how time online can affect sleep, mood and physical activity. Check copyright and permissions before downloading or reusing material. |
| **Year 6** |
| Explain how online friendships can support face-to-face friendships and when time online can get in the way. Evaluate who created a post, why it was targeted and whether it is trustworthy, including where AI may have altered an image. Explain why social media, games and gambling services have age restrictions.<br>Apply privacy and location settings. Explain rights over personal data and ask permission before sharing or tagging others. Recognise that words or pictures can be copied beyond the sender's control. Practise responding to malicious messages, harassment or pressure to share an image, and seeking help for yourself or someone else. |