



2BeSafe Parent Information: Privacy and Security

Introduction to 2BeSafe

At school, we help children learn how to stay safe in today's fast-changing digital world through 2BeSafe, a programme created by 2Simple on Purple Mash. Based on the national Education for a Connected World guidance, 2BeSafe covers eight key areas that prepare children for life online. From Reception to Year 6, children take part in short sessions across the year, giving them clear teaching points and time to reflect and discuss their digital choices.

Privacy and Security

When children go online, they might share personal information without realising how it might be used. This strand teaches them what personal data is, how it can be shared, and why it needs protecting.

From the early years, children learn what information is safe to share and who with, before moving on to topics such as passwords, privacy settings, app permissions, and connected devices.

By Year 6, they are developing strategies to manage data responsibly – creating strong passwords, spotting scams, keeping software updated and recognising what privacy terms and conditions are.

What the Children will be Learning:

Reception: Children learn to recognise simple examples of personal information, such as their name, age, or birthday. They begin to understand who they can safely share this information with and why it is important to trust those people.

Year 1: Children are introduced to the idea of passwords and how they help protect information, accounts, and devices. They learn to recognise more detailed personal information, such as where they live or go to school, and are taught that they should always ask a trusted adult before sharing any of this online.

Year 2: Children develop their understanding of passwords and learn rules for keeping personal information private. They talk about what it means for something to be “private,” practise creating and protecting passwords, and learn that many devices in the home are connected to the internet, such as toys, TVs, or even fridges.

Year 3: Children practise simple strategies for creating and keeping passwords secure. They discuss why information should only be shared with people they know and trust, and that if they feel unsure or pressured, they should always tell an adult. They also begin to understand how connected devices can collect and share personal information.

Year 4: Children explore different strategies for keeping personal information private in a range of situations. They learn that internet use is never fully private and may be monitored. They also begin to understand how online services may ask for consent to collect or store information, what the “digital age of consent” means, and when to ask an adult for help.

Year 5: Children learn what makes a strong password and how to create one. They begin to understand that many free apps and services can collect and share private information, such as contacts, photos, or location. They are also introduced to app permissions and what they mean.

Year 6: In their final year, children learn strategies for managing and protecting passwords, including what to do if one is lost or stolen. They explore why keeping software up to date is important and how privacy settings can increase protection online. They also learn about online scams and phishing, with strategies to recognise and avoid them, and they begin to understand that all online services have terms and conditions that govern their use.



Ways to Support Your Child at Home

- Talk about personal information** – Help your child identify what details are private (such as their full name, address, school, or date of birth) and why they should be protected.
- Model safe sharing** – Show that you also think before posting photos or personal details online.
- Teach about passwords** – Encourage your child to create strong, memorable passwords and explain why they should never be shared with friends.
- Check devices together** – Explore privacy settings on apps, games, and devices, and show your child how these can help keep information safe.
- Discuss app permissions** – When downloading apps, talk about why they ask for access to photos, contacts, or location, and decide together whether this is appropriate.
- Explain online scams** – Teach children that some messages, links, or emails are designed to trick people into giving away money or information. Show them how to spot suspicious content.
- Highlight the importance of updates** – Remind children (and model yourself) that keeping apps and software updated helps protect against security risks.
- Keep conversations open** – Let your child know they can always come to you if they feel unsure or pressured to share information, or if they've clicked on something by mistake.