Lilleshall Primary School

Acceptable Use Policy

Updated: Summer Term 2023
Presented to staff: Summer Term 2023
Reviewed: Summer Term 2026
Next Review: Summer Term 2028

Acceptable Use Policy

- All users should log on with their own username and password.
- You should not share your password with anyone else.
- Always lock your computer if you are moving away from it (Ctrl+Alt+Del then press K).
- We should always think carefully about what we write making sure we always remember to be polite and considerate.
- Remember you are responsible for any communication sent from your account.
- If you come across anything that makes you feel uncomfortable or that you feel you should not have viewed report it to your class teacher straight away or if you are an adult report it to the Head Teacher and ICT services.
- We will not the use the computers for personal financial or political gain (selling, gambling, lobbying etc).
- Remember not all Internet resources are free. We will make sure that before sharing content we have credited sources and checked copyright.
- Any attempt to bypass security systems is a serious offence.
- The school monitors all users of the network, including access to websites. Monitoring is triggered when a violation of this policy is registered on the system.

As a school we agree to follow the SMART rules

- Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.
- Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
- Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
- Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family

- Tell your class teacher or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

How are children are Safeguarded from harmful/inappropriate material online?

Internet Safety is a high-profile area within school and children receive at least one tailored lesson each half-term. This usually takes place the week before a holiday, as the Subject Lead and staff feel this is when children will be most vulnerable to the risks of being online.

We use Project Evolve to establish cohort specific needs by completing class 'Knowledge Maps'. The results of these then inform teacher's planning and highlight the particular strands which they will need to work on. There are eight strands which link with the 'Education for A Connected World Framework':

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership

The required knowledge for each year group is outlined in the subject progression grid.

E-Safety Team are using a training platform called Childnet Digital Leaders. This programme will be used to equip the team with the required knowledge and skills to confidently discuss internet safety with their peers. The team also prepare for the Internet Safety Week and provide updates monthly in an assembly for peers.

Internet Safety Monitoring and Filtering Systems

We use a product called Smoothwall for our internet filtering. This filters internet access for all school devices when onsite, and additionally for computers when offsite.

This filter is differentiated it offers one level of restrictions for students and another for staff, on computers the level provided is based on the login being used. For iPads these are all set to student level, and for the inbuilt Lux system on the Clevertouch screens, this is set to staff level.

Smoothwall filters the internet based on regularly updated categories, we currently offer an enhanced level of filtering that goes above and beyond what is required by Ofsted. We can also filter websites at a domain level, and at a keyword level too.

The default categories are set by T&W, but schools are free customise this as required, along with the domain and keyword filtering.

As an example, we have unblocked the Online Games category for students to allow access to educational online games, and we have unblocked Social Media category for staff to allow access to educational

resources shared on Facebook and Instagram. We also block the amazon.co.uk and amazon.com domains for students.

We also use a product called Senso for monitoring. This software monitors all school computers for potential safeguarding issues, it monitors keystrokes and onscreen content against a list of regularly updated keywords and URLs for violations. If anything is detected a screenshot is taken and is catalogued. Any serious violations generate alert emails which are send to designated school staff (the headteacher). This software also provides application logs and website logs providing a full audit of everything that is done on the computer.

Keywords and URLs can also be modified by the school as required. For example, we currently whitelist the CPOMS URL to not trigger violations when staff are updating CPOMS.

Senso also allows us to monitor all computers as they are in use, all teachers have access and training to Senso to monitor any computer where a student is logged in.