# Internet Acceptable Use Policy

## Lawdale Junior School

**September 2026**

# Internet Acceptable Use Policy

**Rights Respecting Articles**

***Article 6*** *– survival and development. Every child has a right to life. Governments must do all they can to ensure that children survive and develop to their full potential.*

*Article 17 -You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need.*

*Article 19 – protection from all forms of violence. Governments must do all they can to ensure that children are free from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.*

*Article 28---You have the right to a good quality education. You should be encouraged to go to school to the highest level you can.*

*Article 29 – goals of education. Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures and the environment.*

**Policy aims:**

1 To ensure that staff and pupils make use of the Internet for appropriate and educational purposes. This is the use of e-mail, the World Wide Web (WWW) and educational conferencing forums.
2 To ensure that the on-line activity is monitored and managed appropriately.
3 To ensure that staff and pupils are protected from websites, information and individuals that could undermine the principles and aims of the school.
4 To provide a framework of rules that are consistent and in agreement with the Data Protection Act.

**Using the Internet:**

- The Internet may be used for *professional and educational purposes only*.
- When used in the classroom or the ICT suite to support curriculum teaching, the teacher or responsible adult *must* ensure that the children are monitored effectively *at all times*.
- Teachers must *plan* for using the Internet with children and *check* prior to the lesson that any material is not biased, inaccurate, unsuitable or out of date.
- Do not disclose personal details (ie addresses, telephone numbers) of any adult working at the school, pupil, any governor or LEA personnel – school datafiles must be sent securely using USO-FX or another secure data transfer system.
- Be aware of your audience when publishing on the school website or sending e-mails.
- Do not open e-mail attachments when the sender is unknown.
- Never use image searching websites (ie. Google Images) with the children as unsuitable images cannot be filtered. Always save images prior to showing them to the children.
- You Tube and similar video sites may be used to support teaching but the materials must be viewed and planned for prior to the lesson. Searching video hosting websites during a lesson is not permitted under any circumstance and children must not be allowed to browse videos or use the search options for any reason at any time.

# Internet Acceptable Use Policy

All websites visited and all on-line activity, including the use of e-mail, is logged and can be accessed to ensure that this policy is being adhered to at all times.

**Digital images:**

- Only school equipment can be used to take photographs of children to support work within the classroom - for example during model making or during a science investigation to show work in progress.
- Photographs published on the school website must comply with school policy (and parental permission) – no child must be shown on their own and identifiable by name.
- Personal digital cameras and telephones should not be used in the classroom to take photographs of the children without permission of the Headteacher or Deputy Headteacher.

**Restrictions:**

- Pupils may only use e-mail facilities providing it is part of a planned unit of work.
- The forwarding of chain letters or SPAM e-mail messages is forbidden.
- Any e-mail messages sent on behalf of the school must be approved by the senior management team before sending, as is the case for all external communications.
- Any material intended for publishing on the web should also be checked by the senior management team to ensure the acceptable use policy has been adhered to and that no material is subject to copyright.
- The use of chat rooms is not allowed except where a messaging service is used solely within the school network.
- File sharing, such as video and MP3 music files, is illegal and must not take place.
- Video and audio files should not be downloaded unless they are to be used for teaching purposes.
- Programs must not be downloaded and/or installed without permission.
- Accessing user groups and newsgroups is not allowed unless it is an *approved* educational group.
- Users must not upload, download or view inappropriate material, including that of a violent, extremist, dangerous, racist or sexual nature.
- No passwords should be disclosed to anyone (including supply teachers) other than persons responsible for running and maintaining the system.
- Children may not be logged onto the network using a teacher account.

**eSafety:**

Children should be reminded about eSafety in every lesson prior to using any computer or tablet connected to the Internet. eSafety reminders are shown on all computers and on posters around the building. eSafety is also regularly discussed in assemblies, during national awareness weeks and in parents' meetings.

**Social media:**

- The use of social media sites is prohibited for pupils.
- Teachers and support staff need to ensure that comments and images on social media sites do not bring the school or teaching profession into disrepute.
- Social media accounts should be set to private or 'friends-only' so that pupils (former and current) cannot access personal accounts without being invited or having permission.

# Internet Acceptable Use Policy

**Artificial Intelligence (AI):**

As AI tools become increasingly available in education settings, Lawdale Junior School recognises both the potential benefits and the associated risks. AI has the potential to enhance teaching, learning, and workload efficiency when used appropriately; however, its use must be carefully managed to ensure pupil safety, data protection, and ethical practice. AI tools may be used in school for educational and professional purposes only.

**Staff use:**

- Staff are permitted to use AI to support planning, administrative tasks, development of learning resources, assessment, and workload reduction, provided tools are used responsibly and in accordance with GDPR.
- Staff must ensure all AI-generated content is reviewed for accuracy, bias and appropriateness and compliance with curriculum objectives before being used or shared with pupils.
- Staff must be alert to the potential misuse of AI by pupils, including the creation of 'deepfake' content or other forms of AI-generated abuse. Any use of AI to harass, impersonate or bully others will be treated as a safeguarding incident, in line with the school's behaviour and anti-bullying policies.
- Staff must **not** input any personal, confidential, or identifiable information about individuals or proprietary school data into external AI platforms.
- AI must not be used for sensitive decision-making (e.g. disciplinary, safeguarding, employment or medical).
- Staff must be alert to intellectual property issues – AI inputs/outputs must not infringe copyrights or use pupil work without proper consent.
- AI access is subject to filtering and monitoring protocols. If an AI tool is required for educational purposes but blocked, staff must seek authorisation from the Computing Lead.
- Teachers are expected to model responsible AI use and will receive training and CPD to ensure they understand both the benefits and potential risks.
- Staff should not use AI to produce summative reports or feedback unless it is carefully reviewed and adapted to reflect the teachers' own judgement.
- The Computing Lead will regularly update staff on best practices, ethical use, and developments in AI as part of the school's digital strategy.

**Pupil use:**

- Pupils may only use AI tools under direct adult supervision as part of a structured lesson.
- Pupils must not use AI tools to create or share harmful content, including 'deepfake' content that could cause distress or embarrassment to others. Using AI to impersonate, harass or bully others in any way — online or offline — is strictly prohibited and will be treated as a serious safeguarding concern, in line with the school's behaviour, anti-bullying, and online safety policies.
- They must **not** input any personal, confidential, or identifying information about themselves or others.
- AI output must be reviewed for accuracy and suitability, and should not replace pupil effort – original work is required.
- Pupils must be taught to question and verify AI-generated content for accuracy and bias.

- Teachers should ensure students understand how to responsibly use, credit and verify AI-generated content.
- Pupils must acknowledge any use of AI in their work, noting the tool and prompt used.
- To support pupil understanding, the Computing Lead delivers regular assemblies on the responsible use of AI, online safety, and emerging technological developments, ensuring pupils are educated about both the benefits and risks of AI.

**Filtering:**

The school has equipment that restricts access to many websites that it deems as non-educational or inappropriate. This is to prevent children accessing or viewing undesirable material. The URLs, or website addresses, of Internet sites can be added to or removed from this filtering service. If a website is blocked and is needed as part of a unit of planned work or the need to access a restricted website is justified, then the Headteacher or Deputy Headteacher may allow access.

**Breaches of the policy:**

Internet users covered by this policy include the entire school community, namely pupils, governors, teachers and all non-teaching staff. Breaches of this policy, implemented by the Governing Body of the school, could result in one of the following, depending upon the severity and nature of the offence:

- A verbal warning
- Restriction of service or access to ICT resources
- Removal of e-mail facilities and access
- Report to the Governing Body which may result in disciplinary procedures
- Report to the police or other external agencies

And specifically, in the case of children:

- Access only when working alongside an adult or internet restriction
- Letter home to parents

**We will use in our curriculum planning: "Teaching online safety in school" DFe 2019**
This is non statutory guidance and outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It applies to all local authority maintained schools, academies and free schools.
The guidance stresses the importance of teaching pupils about the underpinning knowledge and behaviours that can help them navigate the online world safely and confidently, regardless of the device, platform or app.
Specifically it details:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Understanding what acceptable and unacceptable online behaviour look like
- How to identify online risks
- How and when to seek support

# Internet Acceptable Use Policy

Staff and parents at Lawdale Junior School need 'an understanding of the harms and risks that exist online so we can tailor teaching and support to the specific needs of pupils.' The guidance lists the following issues facing pupils, provides teaching suggestions and details where these could be covered within the curriculum area:

- Age restrictions: Inappropriate content
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data: the gathering of - referred to as ‘harvesting’ or ‘farming’.
- Persuasive design - many devices/apps/games are designed to keep users online for longer than they might have planned or desired.
- Privacy settings
- Targeting of online content
- Abuse (online)
- Challenges: some can be explaining to pupils it's okay to say no
- Content which incites violence
- Fake profiles: Not everyone online is who they say they are
- Grooming: Knowing the different types of grooming
- Pornography: presents a distorted picture of sexual behaviours
- Unsafe communication: Knowing different strategies for staying safe
- Impact on confidence (including body confidence): Knowing about the impact of comparisons to ‘unrealistic’ online images
- Impact on quality of life, physical and mental health and relationships: finding a balance
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders

As with any safeguarding lessons or activities, it is important that schools consider the topic they are covering and the potential that a child/children in the class may be suffering from online abuse or harm in this way. The guidance states 'it is important to create a safe environment in which pupils feel comfortable to say what they feel'.

If we are already aware of a child who is being abused or harmed online we will carefully plan any lesson to consider this, including 'not drawing attention to that child in a way that would highlight or publicise the abuse.'

We will include the Designated Safeguarding Lead (or a deputy) 'when considering and planning any safeguarding related lessons or activities (including online) to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.'

The guidance recommends a number of areas schools should consider, for example how to support vulnerable pupils. Vulnerable Children in a Digital World - Internet Matters is one of several information sources listed that is particularly helpful.
**Teaching online safety in school** also recommends that schools embed teaching about online safety and harms within a whole school approach. In practice, this means:

- Creating a culture that incorporates the principles of online safety across all elements of school life
- Proactively engaging staff, pupils and parents/carers
- Reviewing and maintaining the online safety principles
- Embedding the online safety principles
- Modelling the online safety principles consistently

Throughout the guidance readers are signposted to the Education for a Connected World Framework which includes age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives, including how to navigate online safely.
A copy of **Teaching online safety in school** can be downloaded at:

https://www.childprotectioncompany.com/CPC/media/Teaching_online_safety_in_school.pdf

Also see the school's Safeguarding and Child protection policies and Keeping Children Safe in Education (updated every September).

**Youth Produced Sexual Imagery in accordance with UKCIS's non-statutory guidance, Sharing Nudes and Semi-Nudes. Advice for Education Settings working with Children and Young People 2020.**

**Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.

If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
**Do not** delete the imagery or ask the young person to delete it.
**Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
**Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
**Do not** say or do anything to blame or shame any young people involved.
**Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).