Internet Safety and Acceptable Use Policy

At Lawrence View Primary School the Governors recognise the importance of ensuring equal opportunity for all pupils and adults. The Governors will continue to ensure that this is an essential element of all school policies and actions.
The right to develop, learn and work in an environment free from discrimination is implicit in our school's ethos and embodied in its Vision.

This latest update of this policy was approved on November 2021 at the Business Committee

Next review date Autumn Term 2023.

Signed: ________________________ (Chair) Date: ___________________

Nominated SLT member responsible for policy:

Contents

The implementation of this policy will be monitored at regular intervals. Any significant developments in the use of new technologies, new threats to E-Safety or incidents that have taken place will require regular reviews.

Internet use is part of the statutory curriculum which aims to ensure that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

1. Aims

Our school aims to:

- Have processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- Deliver an effective approach to online safety, to protect and educate the whole school community in its use of technology

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety with appropriate staff.

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 (appendix 2)

3.2 The headteacher

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

ICT co-ordinator

The ICT coordinator takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the school behaviour policy
- Updating staff on online safety on a regular basis
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.3 The ICT technician

The ICT technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.4 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the ICT co-ordinator to ensure that any online safety incidents are identified 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

This list is not intended to be exhaustive.

3.5 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 (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 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 (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the 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

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the ICT co-ordinator.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 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. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.
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.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). 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.

It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs.

There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying and identity theft which cannot be controlled by filtering systems.

In recent years, use of the Internet has continued to increase, particularly with the introduction of mobile devices. This is not only for business and personal use, but also for educational purposes. A wealth of educational resources are now available on the Internet and via mobile devices; and this continues to grow. At Lawrence View Primary School, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning. Resources found on the Internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process.

The Internet, by its open and dynamic nature, may lead pupils to material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point pupils to relevant curriculum sites or to previously researched sites that have been identified as being relevant to the area of study, we also accept our responsibility in educating our pupils about responsible, respectful, and safe use of the Internet. Research using electronic methods is now fundamental to preparing pupils for citizenship and future employment.

The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about e-safety will be planned and that staff will guide pupils in line with Government guidelines. The school recognises that training the staff in preparation for using the Internet and indeed any mobile technology in a safe manner is vital.
Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and E-Safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference. The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the ICT co-ordinator. The co-ordinator will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access or attempt to access inappropriate materials. It is anticipated that access to younger pupils will be more directed, with autonomous use being available to older pupils. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, ICT co-ordinator or the Head.

E-safety will form an integral part of computing lessons but will also be covered in regular assemblies and as part of our PSHE programme of study. The school believes that access to the Internet and mobile devices will enable pupils to explore resources in a way that will enhance the learning process in ways impossible by other means.

The school believes that access to this technology brings benefits to the learning processes that outweigh the possible risks that might be encountered. Older children will be encouraged to accept some responsibility for their use of the Internet and will be asked to sign a pupil e-safety declaration. The final responsibility for use of the Internet and E-Safety lies with the parents and guardians of our pupils.

This policy will be reviewed on a regular basis in line with the E-Safety Policy and any technological advances and developments.

8. Pupils using mobile devices in school
Many children have mobile phones which are part of their daily lives, enabling contact with parents or carers on the journey to and from school. Children in Key Stage 2 are allowed to bring mobile phones into school however these are to be turned off and stored in the teacher’s desk drawer throughout the school day. As a personal possession, a mobile phone is not the responsibility of the school at any time.

Teachers have the legal right to examine any data or files on a child’s mobile phone if they think there is a good reason to do so, for example (but not exclusively) if bullying or safeguarding issues are suspected. The school is not required to inform parents or carers before a search takes place or to seek their consent. Out of courtesy, the school will inform the parent or carer should such an examination take place, although this is not a requirement by law. If inappropriate or offensive material is found on the device it is up to the Head Teacher to decide whether they should delete that material, retain it as evidence

(Of a criminal offence or a breach of school discipline or whether the material is of such seriousness that it requires the involvement of the police). Other digital devices are not permitted to be brought to school.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Work devices must be used solely for work activities.

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 the behaviour 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. 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, e-bulletins, and staff meetings).

The DSL 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. More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaint’s procedure
- Prevent policy