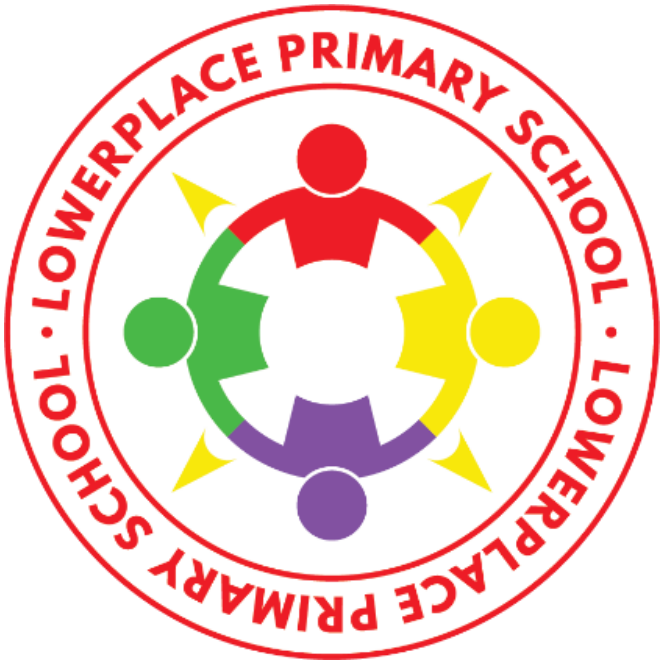

E-Safety Policy

Adopted: 02/2021

Reviewed March 2024

1. Aims

Our school aims to:
Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

It also refers to the DfE's guidance on protecting children from radicalisation

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

3. Roles and responsibilities

3.1 The governing board

All governors will:

- Ensure that they have read and understand this policy
- Ensure that the school follows all authoritative E-safety advice to protect the welfare of pupils and staff
- Approve the E-safety Policy and regularly review the effectiveness of this policy
- Support the school in encouraging parents and the wider community to become engaged in E- safety activities
- Undertake appropriate training and development on E-safety issues.

3.2 The headteacher

The headteacher will:

- Take overall responsibility for the provision of online safety
- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensure the school uses an approved, filtered internet service, which is fully compliant with current statutory requirements
- Be responsible for ensuring that staff receive suitable training to carry out their E-safety roles
- Ensure that robust systems are in place to monitor and support staff who carry out internal E- safety proceduresThe designated safeguarding lead

3.3 The designated safeguarding lead

Details of the school's DSL are set out in our Safeguarding and Child Protection policy as well as relevant job descriptions.

The DSL will:

- Work with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and delivering staff training on online
- Liaise with other agencies and/or external services if necessary
- Regularly update their own knowledge and understanding of E-safety issues and legislation (and to cascade this to other staff) and remain constantly aware of the potential for serious child protection issues

3.4 The ICT manager/Technician

The ICT manager 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
- against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

3.5 All staff and volunteers

All staff 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Model safe, responsible and professional behaviours in their personal use of information technology

3.6 Pupils

Pupils are expected to:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials or sites
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Have a good understanding (appropriate to their age and abilities) of research skills and the need to avoid plagiarism and uphold copyright regulations

3.7 Parents/Carers

Parents are expected to:

- Read, understand, sign and adhere* to the Pupil Acceptable Use Agreement
- 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 (appendices 1 and 2)

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

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

5. Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Google Classroom. 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 DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Education, internet and the curriculum

The school provides repeated opportunities (within a broad range of curriculum areas) to learn about E-safety and before using the internet pupils will be made aware of the relevant legislation such as data protection and intellectual property rights.

6.1 Pupils are also given advice if they experience problems whilst using the internet and/or email and are provided with guidance on promoting E-safety including the requirements to:

- understand the importance of misuse (including accessing inappropriate materials or sites) and are aware of the consequences of this
- understand how to ensure their privacy settings are appropriately configured and to know why they should not post (or share) detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos etc
- understand why they must not post pictures or videos of others without their express consent
- understand issues around plagiarism and how to check copyright etc
- know not to download any files (such as music files) without appropriate permission
- only use approved class email accounts under supervision by (or with permission from) a teacher.

6.2 The 'Pupil Acceptable Use Policy' (Appendix 1 & 2) reminds pupils about their responsibilities and details the strategies to maximise learning opportunities whilst reducing potential risks associated with use of the internet.

7. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes:

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

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 our policies on behaviour and remote learning, 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/staff code of conduct. 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 DSLs 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, as applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

12. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints policy