E-safety Policy

<table>
<tr><th>Version</th><th>Document Title</th><th>Status</th><th>Author</th><th>Approved by</th><th>Date</th><th>Next Review Date</th></tr>
<tr><td>0.1</td><td>E-safety Policy</td><td>Final</td><td>IT Specialist & Head of ICT</td><td>Principal/Vice Principal</td><td>August 2024</td><td>August 2025</td></tr>
<tr><td colspan="2">Regional Director</td><td colspan="3">Principal</td><td colspan="2">Vice Principal</td></tr>
<tr><td colspan="2">Head of Foundation Stage</td><td colspan="3">Head of Primary</td><td colspan="2">Head of Secondary</td></tr>
</table>

1. Aim

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

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate

The three key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as fake news, racism,
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images and online bullying

2. Roles and responsibilities

2.1 The governing board

The governing board monitors this policy and holds the principal accountable for its implementation. The governing board will ensure that all staff undergo online safety training as part of child protection and safeguarding training and that staff understand their expectations, roles, and responsibilities regarding filtering and monitoring.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, training requirements, and monitoring of online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught to keep themselves and others safe online. The governing board must ensure the school has appropriate filtering and monitoring systems on school devices and networks and will regularly review their effectiveness. The board will review the filtering and monitoring standards and discuss with IT staff and service providers what needs to be done to support the school in meeting the set standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children and some pupils with special educational needs and disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

2.2 The Principal

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

2.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy,

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

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the principal and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT specialist to make sure the appropriate systems and processes are in place
- Working with the principal, IT specialist and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

2.4 The IT Specialist

The IT specialist is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess the effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school.

- 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 monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially hazardous files
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies or external services if necessary
- Providing regular reports on online safety in school to the principal and DSL
- Undertaking annual risk assessments that consider and reflect the risks children face

2.5 All staff and volunteers

All 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 and ensuring that pupils follow the school's terms on acceptable Working with the DSL to ensure that any online safety incidents are logged 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
- Responding appropriately to all reports and concerns about sexual violence or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

2.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the principal/vice-principal 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.

2.7 Visitors and members of the community

Visitors and community members who use the school's ICT systems or the 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 acceptable use terms.

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

Primary schools

In **Key Stage (KS) 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

In **Key Stage (KS) 2**, pupils 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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary schools

In **Key Stage (KS) 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the exact expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want to be shared further and not to share personal material that is sent to them

- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims and some pupils with SEND.

4. Educating parents/carers about online safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications at home and information via our website. This policy will also be shared with parents/carers.
Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access to.
- If parents/carers have any queries or concerns about online safety, these should be raised in the first instance with the principal and the DSL.

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

5. Cyber-bullying

5.1 Definition

Cyberbullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti- Bullying policy and the school behaviour policy.)

5.2 Preventing and addressing cyber-bullying

To help prevent cyberbullying, 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 also ensure that pupils know how to report incidents and are encouraged to do so, including where they are witnesses rather than victims.
The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take, and the consequences. Homeroom and Form teachers will discuss cyberbullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to address cyberbullying. This includes personal, social, health, and economic (PSHE) MSC education and other subjects where appropriate.
As part of safeguarding training, all staff, governors, and volunteers (where appropriate) receive training on cyberbullying, its impact, and ways to support pupils.

The school will follow the behaviour policy processes concerning a specific cyberbullying incident. 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if necessary.

5.3 Examining Electronic Devices

The principal and any member of staff authorised to do so by the principal can search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils and
- Is identified in the school rules as a banned item for which a search can be carried out and
- Is evidence about an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the principal / DSL.
- Explain to the pupil why they are being searched and how the search will happen, and allow them to ask questions about it
- Seek the pupil’s co-operation

Authorised staff members may examine and, in exceptional circumstances, erase any data or files on an electronic device they have confiscated where they believe there is a ‘good reason’ to do so.
When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm and/or
- Undermine the safe environment of the school or disrupt teaching and
- Commit an offence

Suppose inappropriate material is found on the device. In that case, it is up to the staff member and the DSL / principal/ other senior leadership team member to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence of a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence of an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

- They suspect a device may contain an indecent image of a child (also known as a nude)

The school complaints procedure will handle complaints about pupils searching for or deleting inappropriate images or files on their electronic devices.

5.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easily accessible. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Board.
Newlands School recognises that AI has many uses to help pupils learn but may also have the potential to bully others. For example, in the form of 'deepfakes', AI is used to create images, audio, or video hoaxes that look real.

Newlands School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.
Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where the school is using new AI tools.

6. Acceptable use of the Internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to agree on the acceptable use of the school’s ICT systems and the internet (BYOD Policy digitally signed by students & parents)
The school’s internet must be used for educational purposes only or to fulfil 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 and restrict access through filtering systems where appropriate.

7. Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them during:

- School hours, 7:30am-2:30pm, including CCA time and educational trips

Pupils' use of mobile devices in school must be by the acceptable use agreement (BYOD Policy)
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in confiscating their device.

8. 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 Behavior, Digital Learning and BYOD policies. The action will depend on the specific incident's circumstances, nature and seriousness and will be proportionate.
Where a staff member misuses the school’s ICT systems or the internet or misuses a personal device and 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.

9. Training

All new staff members will receive training on safe internet use and online safeguarding issues, including cyberbullying, as part of their induction.

All staff members will receive refresher training at least once each academic year as part of safeguarding training and relevant updates as required (for example, through emails and staff meetings).
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and well-being issues, and children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and messages
    - Online Bullying

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training every two years, including online safety. At least annually, they will regularly update their knowledge and skills on online safety.

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.

Our child protection, BYOD, Digital Learning, and Safeguarding policies provide more information about safeguarding training.

10. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

The DSL will review this policy annually and share it with the governing board at each review. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology and the risks and harms related to it evolve rapidly.

11. Links with other policies & Documents

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Positive Behaviour policy

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Digital Learning Policy
- BYOD Policy
- Passwords Policy
- Firewall logs
- Web/Application Filtering standards

Appendix 4: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**