	Vanguard Learning Trust *As a group of local primary and secondary schools, Vanguard Learning Trust's mission is to serve its local community by providing outstanding, inclusive education. We have a collective purpose and responsibility to provide effective teaching, through a curriculum based on equality of opportunity and entitlement that allows our students to shine both in and out of the classroom. Each school in the Trust has its own ethos, which also complements the Trust's vision and values, and the common aspiration that all students can achieve their potential.*

Internet Safety Policy
February 2024-2025

Contents

1. Aims

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 internet 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

1.1 The 4 key categories of risk

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

1 **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

2 **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

3 **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

4 **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) 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
Searching, screening and confiscation

It also refers to the DfE'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. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Importance and benefit of the Internet in schools:

- The purpose of Internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and pupils and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st-century life for education, business and social interaction.

- The school has a duty to provide students with quality Internet access as part of their learning experience so that they can gain insight into worldwide resources.
- Staff can develop their professional skills through access to national developments, educational materials and good curriculum practice.

4. How will pupils act online and learn about using the internet?

- Pupils will understand the SMART rules when using the Internet. (Safe, Meeting, Accepting, Reliable, Tell)
- Pupils in Early Years will begin learning about Internet Safety through the Smartie the Penguin programme. Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.
- Pupils in Years 1 – 6 will be taught structured Internet Safety lessons from the PIXL programme. There are separate schemes for Years 1 and 2, Years 3 and 4 and Years 5 and 6. These will be taught throughout the year as an ongoing programme for internet safety.
- Pupils in Years 1 – 6, in the autumn term, will be taught Online Safety through the Purple Mash unit.
- Ensure they are aware of the risks involved with using the Internet and changes that are occurring.
- Pupils must immediately tell a trusted adult if they receive anything offensive online. They should also keep the e-mail until the trusted adult can take evidence of the material.
- Will not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils should use language that is sensible and appropriate. Language which is used to bully or be rude to someone will not be acceptable.
- Pupils should only contact and arrange to meet people they know or those the teacher has approved. Pupils must keep personal details to themselves. These can include: where they go to school, their home address(es), telephone numbers and passwords.

4.1 The curriculum at each key stage

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

Pupils in **Key Stage (KS) 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

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
- How information and data is shared and used online
- 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

5. Roles and Responsibilities:

5.1 How staff will ensure best practice:

- Training will be given to staff in the evaluation of web materials.
- Knowing that the Lead DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing to the DSLs
- Promote the positive use and values of the Internet, including the use of Social Media.
- Ensure they are aware of the risks involved with using the Internet and changes that are occurring.
- Take time to understand and read the policies and procedures put into place, as well as Internet Safety material they may receive.
- Internet safety will be explicitly taught to the pupils**.**
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Inform pupils that their Internet use is monitored in person during lessons as well as via a monitoring platform.
- Ensure that all web-based content shared with pupils during whole-class teaching is age appropriate. Model the use of using "for kids" when using search engines.
- Access to the Internet will be demonstrated by an adult, with directly supervised access to specific, approved online materials.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (LGfL) via the Computing Coordinator or Headteacher.
- Report all Internet Safety issues immediately but not exceeding 24 hours of being alerted to the issue.
- E-mails sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Lead DSL/DSLs.
- 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 and/or harassment, both online and offline, and maintaining an attitude of 'it can happen here'
- Teachers and TAs use the resources provided by National Online Safety.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

5.2 How the Lead DSL will ensure best practice:

- Educate those within the school about Internet Safety and what to do if that safety is compromised.
- Take part in national events, such as Internet Safety Day. IT Coordinator will lead on this.
- Lead DSL to continue to share safeguarding information and guidance to parents via the school's padlet, as well as via the school newsletter.
- If parents/carers 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.
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the headteacher and governing body 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 Coordinator to make sure the appropriate systems and processes are in place.
- Working with the headteacher, IT Coordinator 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 (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body
- Undertaking annual risk assessments/audits that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

5.3 How governors will ensure best practice:

- The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.
- The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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.

The governor who oversees online safety is Ann-Marie Taylor Kent.

5.4 How parents will ensure best practice:

Parents/carers 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 IT systems and internet (see Computing Acceptable Use Policy)

Parents/carers 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
- Parent resource sheet – Childnet
- School's Safeguarding and Wellbeing Padlet

6. How will school online accounts be managed?

- Website photographs that include pupils will be selected carefully.
- Only the first names of children will be used online.
- Photograph permission will be sought from parents/carers via a consent form (as part of the admissions process)
- Teachers will be made aware of those who have not consented to photos.
- The Headteacher or SLT nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

7. How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to the Headteacher or a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaints against the Headteacher must be raised with the Chair of the Governing Body.

8. How will we respond to issues of misuse?

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies: behaviour and internet acceptable use. 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 IT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the trust 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. 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, briefings 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 misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

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 Lead DSL and Deputies 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 (provided by the Trust)
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

10. How will we protect ourselves against cyber-crime?

Cyber-crime is a criminal activity committed using computers and/or the internet. It can involve malicious attacks on computer software, including:

Email hacking
Email hackers try to gain access to email accounts by tricking people to:

- open and respond to spam emails
- open emails with a virus
- open phishing emails

Phishing
Phishing messages look authentic with corporate logos and a similar format to official emails.
Sometimes phishing emails use the title of a genuine email that the victim has recently replied to in order to trick the victim into believing the communication is authentic.
Phishing emails can appear to have originated from within or outside your organisation.
Unlike official communications, phishing emails ask for verification of personal information, such as account numbers, passwords or date of birth.
Sometimes the emails suggest the request is time-sensitive to pressure the recipient to respond when they might not otherwise have done so.
Unsuspecting victims who respond may suffer stolen accounts, financial loss and identity theft.

Malvertising
Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to your computer while the website is still loading in the background. Cyber criminals can use advertisements as a way to hack into computers.

10.1 To address the risk of fraud, theft and/or irregularity, we:

- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access

10.2 We also train staff to ensure that they:

- routinely take part in phishing tasks to ensure skills and knowledge are applied and reviewed
- undertake annual training: NCSC Cyber security training for school staff (LINK), as well as other relevant training via The National College
- check the sender of an email is genuine before, for example, sending payment, data or passwords
- make direct contact with the sender (without using the reply function) where the email, for example, requests a payment or change of bank details
- if telephoning the sender to confirm authenticity, do not use the contact number within the email without first checking it is genuine
- understand the risks of using public Wi-Fi
- understand the risks of not following payment checks and measures

11. Monitoring

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

This policy will be reviewed every year by the IT Coordinator and Lead DSL. At every review, the policy will be shared with the governing body. The review is also supported by an annual online safety audit that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Approval / Revision History

Revision date	By	Summary of Changes Made
February 2023	Siobhan Rowland IT Coordinator	Policy reviewed to new VLT template, wording for Headteacher changed to Headteacher. Early Years update, no other specific new content updates
February 2024	Parmjit Kaur Varaitch Lead DSL	Grammatical errors were amended and additional information was added in yellow highlight. Reference was made to The Key model policy and several additions made.

List of appendices

Appendix 1: Online safety training needs: self-audit for staff

Appendix 1: Online safety training needs: self-audit for staff

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?	
Are there any areas of online safety in which you would like training/further training?	