THE VINE INTER-CHURCH PRIMARY SCHOOL

Online Safety Policy

Policy Development:	Autumn 2021
Policy Ratification:	December 2021
Policy Review:	Autumn 2024

Link to The Vine Vision – Love of Life Itself

This policy demonstrates our commitment to ensuring all members of our school are safe, respectful and responsible internet users. Through our rigorous approach to safeguarding and robust teaching of Online Safety, we provide our pupils with a safe, secure environment as well as the skills and knowledge necessary to utilise the internet and thrive in the digital world in which we live.

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 5
5. Educating parents about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 9
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 9
11. Training 9
12. Monitoring arrangements 10
13. Links with other policies 10
Appendix 1: EYFS and KS1 Acceptable Use Agreement 11
Appendix 2: KS2 Acceptable Use Agreement 12
Appendix 3: Staff Acceptable Use Agreement 13

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, 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 4 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 pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **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
- **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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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
- Relationships and sex education
- 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. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding leads (DSLs).

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 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

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.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL Team take 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 manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the schools Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 Anti-Bullying policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on My Concern 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 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 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
- 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 could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

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 3).

4. Educating pupils about online safety

To ensure that the pupils knowledge of how to use the internet safely and respectful is robust, an Online Safety is taught in every year group. The learning objectives covered in each year group are detailed below.

In the **Early Years Foundation Stage**, pupils will be taught to:

- Know that they need to share with a grown up what they are doing on a device and to ask for help if something isn't right.
- Identify adults inside and outside school that can help if they see something they do not like online.

- Begin to know what personal information is and that it should be kept private.

In **Year One**, pupils will be taught to:

- Identify adults inside and outside school that can help if they see something they do not like online.
- Know that they need to keep the browser open if they see something they do not like but minimise it or hide the screen and tell a trusted adult.
- Know what personal information is and that it should be kept private.

In **Year Two**, pupils will be taught to:

- Identify adults inside and outside school that can help if they see something they do not like online and confidently explain what they have to do to keep themselves and others safe.
- Know which personal information should not be shared online (full name, address, school, usernames, and passwords).
- Begin to explain why personal information needs to be kept private.

In **Year Three**, pupils will be taught to:

- Confidently explain which personal information should not be shared online (full name, address, school, passwords, usernames and any other more specific personal details such as medical information, plans in social life) and why.
- Recognise acceptable and unacceptable behaviour whilst online.
- Define cyberbullying and identify instances of it
- Understand the need of an alias for some online communication.

In **Year Four**, pupils will be taught to:

- Identify some of the potential online risks of inappropriate contact or content.
- Know how to respond if asked for personal information or feel unsafe when communicating with others online.
- Confidently explain some of the ways other users might use their personal information.
- Know you should open messages or attachments from a known source.
- Understand how to create a secure password.
- Understand how communication online may be seen and used by others and that once posted the sender has lost control of it

In **Year Five**, pupils will be taught to:

- Identify a fuller range of the potential online risks of inappropriate contact or content and the effect on self-image and reputation.
- Identify additional ways of seeking support and reporting concerns about content or contact.
- Understand their rights and responsibilities when communicating online and how their actions may affect others.
- Begin to understand the use and abuse of social media.

- Understand and explain the concept of their digital footprint, how it can be tracked and used by others.
- Begin to understand and use online safety and security settings.

In **Year Six**, pupils will be taught to:

- Confidently identify and explain potential online risks of inappropriate contact or content and the effect on self-image and reputation.
- Confidently explain the range of ways to report concerns.
- Understand and explain the potential risks of social media and the means by which you can avoid inappropriate behaviour.
- Understand and use safety and security settings.
- Confidently explain their rights and responsibilities when communicating online and how their actions may affect others.
- Understand the consequences of inappropriate behaviour online, especially on social media and in online gaming.

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 DSL.

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. (See also the school behaviour policy.)

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.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

Pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils are not allowed access to their mobile devices whilst on the school site. Any mobile devices brought into school are stored in a secure place by a member of staff at the beginning of the school day. The device is returned to the pupil at the end of the day and must not be used until they have left the school site.

If a pupil uses their phone during the school day, it will be confiscated and a sanction will follow. Repeated breaches will result in the phone being returned only to a guardian, who will be required to visit the school by appointment to collect the phone.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- 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)
- 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

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 ICT 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 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, 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 the risks up
- 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 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.

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. Monitoring arrangements

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

This policy will be reviewed every year by the Computing and Online Safety Lead. At every review, the policy will be shared with the governing board. The review 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 and change rapidly.

13. 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
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 Acceptable Use Agreement

Rules for Responsible Computer & Internet Use

At the Vine School, you will have the chance to use lots of resources such as Computers, iPads, the internet and much more!

It is important that you follow the rules below to make sure that you can stay safe, be fair to others and take care of our equipment.

1. I will only log into the computers using my own year group log in.
2. I will only use the internet and print work once my teacher has given me permission.
3. I will keep my personal information private.
4. I will not log into my personal accounts in school.
5. I will get help from an adult if I see something on the internet which makes me feel worried, scared or sad.
6. I will take care of the equipment and never damage it on purpose.
7. I will not eat or drink near any computer equipment.

I understand that if I break these rules, I will not be allowed to use the Computing resources.

Full name: _____ Date: _____

Appendix 2: KS2 Acceptable Use Agreement

Rules for Responsible Computer & Internet Use

At the Vine School, you will have the opportunity to use a variety of IT resources, equipment and services to help you with your learning. Whilst doing so, it is important that you follow the rules below to keep everyone safe, be fair to others and take care of our equipment.

- I will only log in to the computer systems using my own year group username and password.
- I will not access any files other than my own unless I have been given permission by a teacher.
- I will not use school computers to read SD cards or USB devices from outside school unless I have been given permission by my teacher.
- I will ask permission from a teacher before printing anything.
- I will ask permission from a teacher before using the internet.
- I will use the internet safely and responsibly, only searching for and viewing appropriate websites and images.
- I will not access any personal accounts on school laptops or iPads.
- I will keep my personal information private and never arrange to meet someone online unless my parent/ carer has given me permission.
- I will tell my teacher if I see or read any unpleasant material or messages online.
- I understand that the school will check my computer files and will monitor the sites that I visit.
- I will respect school equipment and not intentionally cause it to be damaged.
- Food and drink must never be consumed at or near any computer equipment.

I understand and accept that if I break these rules my computer access will be withdrawn.

Full name: _____ Date: _____

Appendix 3: Staff Acceptable Use Agreement

Rules for Responsible Computer & Internet Use

The computer system is owned by the school and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited. School email accounts are owned by the school and can be accessed by the head teacher at any time.

Staff requesting internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Computing Lead, Gemma Gray, for approval.

- Computers are to only to be used for work purposes and not for private use.
- All internet activity should be appropriate for staff professional activity or the pupils' education.
- Personal accounts for social media sites should not be accessed using school computers or iPads.
- Access to the network should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school computer network, or activity that attacks or corrupts other systems, is forbidden.
- Computers must be locked (⊞ + l) when left unattended.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- Copyright of materials must be respected.

- Posting anonymous messages and forwarding chain letters is forbidden.

- As e-mails can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

- Passwords should be at least ten characters long containing capital letters, numbers and symbols and should not be used across multiple platforms. These must not be set to autosave.

- No food or drink should be consumed near computers or iPads.

Full name: _____

Signed: _____ Date: _____