Online Safety Policy

2024-2025

Person responsible for the policy	**Computing Lead: Hirra Zahid**

Aims and policy scope

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Vicarage Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

- Vicarage Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- Vicarage Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- Vicarage Primary School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- Vicarage Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Vicarage Primary School's online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Vicarage Primary School is a safe and secure environment. Safeguard and protect all members of Vicarage Primary School community online.
- Raise awareness with all members of Vicarage Primary School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, tablets or mobile phones.

Links to other policies and national guidance

The following school policies and procedures should also be referred to Safeguarding & Child Protection Policy Whistleblowing policy

Positive Behaviour Policy
Anti-Bullying Policy
Acceptance Use Policy
Guidance on Safer Working Practice
Staff code of conduct
Data Protection
Personal Social and Health Education (PSHE), Sex and Relationships Education (SRE) Policy

The following local/national guidance should also be read in conjunction with this policy:

Newham Local Safeguarding Children Partnership, Guidelines and Procedures (2019)
PREVENT Strategy HM Government

Keeping Children Safe in Education DfE
Teaching Online Safety in Schools DfE
Working together to Safeguard Children

Reviewing and Monitoring

Vicarage Primary School online safety policy has been written by the online safety lead, involving staff, pupils and parents/carers, with specialist advice and input as required.
The policy has been approved and agreed by the Leadership team and Governing Body

The online safety (eSafety) Policy and its implementation will be reviewed by the school at least annually or sooner if required.

Communication

The policy will be communicated to staff/pupils/community in the following ways: Policy to be posted on the school website/ staffroom.

Policy to be part of school induction pack for new staff.

Acceptable use agreements discussed with pupils at the start of each year.

Acceptable use agreements to be issued to whole school community, usually on entry to the school

Acceptable use agreements to be held in pupil and personnel files

Key responsibilities

The Designated Safeguarding Lead (DSL) is Shabana Khan
The Designated Online Safety Lead (DOS) is Hirra Zahid

Leadership team

- To take overall responsibility for e-Safety provision
- To take overall responsibility for data and data security GDPR compliant
- To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg. LGfL
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
- To be aware of procedures to be followed in the event of a serious e-Safety incident. To receive regular monitoring reports about E-Safety from Computing Lead
- To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures

E-Safety Lead and Designated Safeguarding Lead are:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- promotes an awareness and commitment to e-safeguarding throughout the school community
- ensures that e-safety education is embedded across the curriculum liaises with school COMPUTING technical staff
- To communicate regularly with SLT and the designated e-Safety

- Governor / committee to discuss current issues, review incident logs and filtering / change control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- To ensure that an e-Safety incident log is kept up to date facilitates training and advice for all staff
- liaises with the Local Authority and relevant agencies
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults/strangers potential or actual incidents of grooming
- cyber-bullying and use of social media

Governors

- To ensure that the school follows all current e-Safety advice to keep the children and staff safe
- To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub
- Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Computing Curriculum Lead

- To oversee the delivery of the e-safety element of the Computing curriculum To address e-safety issues as they arise promptly

IT Technician

- To report any e-Safety related issues that arises, to the Computing Coordinator.
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)
- To ensure the security of the school Computing system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- The school's policy on web filtering is applied and updated on a regular basis LGfL is informed of issues relating to the filtering applied by the Grid
- To keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the network / remote access / email/School Twitter account is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator/Data Protection
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's e-security and technical procedures

Data Protection Lead/ Data Protection Officer

- To take overall responsibility for data and data security
- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

All members of staff

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them. Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site. Demonstrating an emphasis on positive learning opportunities.
- To maintain an awareness of current e-Safety issues and guidance e.g. through CPD
- To read, understand and help promote the school's e-Safety policies and guidance
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils

- Read, understand, sign and adhere to the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home

Parents / Carers

- To support the school in promoting e-safety and endorse the Parents'
- Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images

- To read, understand and adhere to the school Twitter policy
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To access the school website /Twitter account accordance with the relevant school Acceptable Use
- Agreement.
- To consult with the school if they have any concerns about their children's use of technology

Teaching & Learning

Online Communication and Safer Use of Technology

Online Learning platforms

- In response to COVID-19, the school has adopted the use of educational sites to deliver the curriculum. Google Classroom has been adopted throughout the school from EYFS-Y6. The following points are related to the use of Google classroom
- All students will be given a Gmail login to access our system servers and the intranet and internet in school. With school Gmail and Google Docs, for example, work and emails cannot be shared with external email accounts, only with others within @viacarage.newvisiontrust.co.uk - the school's Google domain. Google requires basic information to set up these accounts, which have been taken from SIMS and consented to in the application form.
- Pupil accounts have a particular set of security settings to reflect the fact that the system is being used by a child
- Pupils can only access and comment on classrooms allocated to them and the teachers can restrict comments where required.
- Teachers can monitor activity online including usage, downloads and comments. Teaching drive is only accessible by staff.
- Teachers will upload any Youtube videos and other attachments as opposed to publishing the link to avoid any inappropriate adverts appearing.
- Google accounts are deleted within a few weeks of a child leaving and for all Year 6 pupils.
- Any live sessions completed must be done so with reflection to the safeguarding policy including but not limited to: sessions completed in open spaced living rooms (not bedrooms), no personal information visible in the live stream, with a minimum of 3 or more children otherwise the sessions are terminated. All live session meeting links are posted 10minutes prior to the session and teachers are required to enquire if everyone leaves the meeting before ending the meeting.
- Recorded sessions are available for up to a week before these expire and children cannot access them again.
- Google Classroom online firewall as part of the G-Suite package. This also restricts access to websites, certain words and phrases in searches, access to student friendly videos on youtube.com

Google's Privacy Policy for GSuite can be found here: https://policies.google.com/privacy/update

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publicationsincluding accessibility, respect for intellectual property rights, privacy policies and copyright.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- Pupils' work will be published with their permission or that of their parents/carers.

- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.

Managing email

- Pupils may only use school provided email accounts for educational purposes
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Excessive social email use can interfere with teaching and learning and will berestricted. Access in school to external personal email accounts may be blocked.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Google Classroom online firewall as part of the G-Suite package. This also restricts access to websites, certain words and phrases in searches, access to student friendly videos on youtube.com
- Tracking of pupil's activity on the internet within school lessons using Smoothwall filtering and monitoring service a specific monitoring software package, where any incidents and flags will be sent to the Safeguarding team.

- Supervision of pupils will be appropriate to their age and ability
- At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. All teaching staff are to be assigned iPads to used in a professional manner and used for educational purposes. Each allocation will be recorded and monitored to ensure safety guidelines are respected and adhered to.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools (Safesearch) as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Filtering and monitoring

The school:

- Has the educational filtered secure broadband connectivity through the SWGfL and also connects to the 'private' Google Apps for Education domain
- Uses the SWGfL Net Sweeper filtering system, which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' statu
- Ensures networks remain healthy through use of Sophos anti-virus software (from SWGfL) etc. and network set-up so staff and pupils cannot download executable files
- Uses DfE, LA, Google Apps for Education domain or SWGfL approved secured email to send personal data over the Internet and uses encrypted devices, secure remote access or Google Apps for Education where staff need to access personal level data off-site
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level
- Uses security time-outs on Internet access where practicable / useful

Management of school learning platforms/portals/gateways

- Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP will be recorded and dealt with in the following ways: The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply. Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Social Media Policy Official use of social media

Vicarage Primary School currently has a Twitter account. Following expectations are required to be adhered to:

- Only SLT members will tweet pre agreed tweets.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Vicarage Primary School's community.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications e.g. google classroom
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils / parents / carers or school staff
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (Staff email)
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby the Headteacher has given prior approval.
- They do not engage in online discussion on personal matters relating to members of the school community

- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Use of Personal Devices and Mobile Phones
Student personal use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via online safety and safer internet day, age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Mobile phones and personally -owned devices will be switched off or switched to 'silent' mode,

CCTV

The school may use CCTV in some areas of school property as a security measure.

Cameras will only be used in appropriate areas and as an investigative avenue for any incidents that arises.

Managing Information Systems

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing leader/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.

- All users will be expected to log off or lock their screens/devices if systems are unattended. Password policy
- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From year 2, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff to change their passwords every 90 days and there are systems in place to enforce this.

Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information.
- All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact.
- Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded on Safeguard.
- The school also reserves the right to report any illegal activities to the appropriate authorities
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local
- Authority Designated Officer).
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Appendix A Online Safety (e-Safety) Contacts and References

National Crime Agency:
https://www.ceop.police.uk/safety-centre/
Metropolitan Police:
http://content.met.police.uk/Borough/Redbridge
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Metropolitan Police via 101

National Links and Resources

Action Fraud: www.actionfraud.police.uk BBC WebWise: www.bbc.co.uk/webwise CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Tootoot: www.tootooot.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/ Filtering tool: https://www.netsweeper.com/solutions-centre/education/ofsted/