Internet Acceptable Use Policy

Viridis Schools

May 2026

To be reviewed 2027 or as required

Context

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within our schools. This policy should be read in conjunction with the Safeguarding Policy and ICT Policy. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate new developments.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

- The steps taken in school to ensure the safety of pupils when using the internet, e-mail and related technologies.
- The school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school.
- The school's expectations for the behaviour of staff when accessing and using data.

The school reserves the right to monitor usage of the network, and pupils and staff should be aware that routine monitoring takes place.

Aims

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of the school community.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

The school

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Will ensure that all staff are aware of the acceptable use policy and that e-safety and the reporting of concerns is integrated into our school curriculum.
- Does not allow pupils to carry mobile telephones whilst the school is in session and that these are kept in the school office.
- Ensures pupils only publish within the appropriately secure school's learning environment, such as Google Classroom.
- Requires staff to preview websites before use [where not previously viewed or cached].
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search.
- Informs users that Internet use is monitored.

- Informs staff and pupil that that they must report any failure of the filtering systems directly to the ICT technician and or Headteacher. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGfL (Atomwide) as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable and in-line with the school behaviour management system.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents.
- Provides online safety advice for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities.

Acceptable Use Expectations

E-mail

- All e-mails must be polite, factual and use appropriate language. In particular they must not contain any material that could be considered derogatory, abusive, sexist, racist, incite hatred or opinion led.
- E-mails should not reveal personal details, whether about the sender or someone else.
- Any pupil or staff member receiving an abusive or offensive e-mail should inform their teacher or line manager immediately, such emails must not be responded to.
- Pupils and staff should not engage in 'spamming' or participate in chain e-mails.
- Social and work e-mail is strictly forbidden during lessons without explicit permission.
- E-mails sent to external recipients on behalf of our schools must be carefully written and checked BEFORE sending.
- The use of e-mail for social purposes should be kept proportional to the primary academic purpose.

Online Meetings / Remote Conferencing

In order to create a safe environment for pupils and staff when taking part in any remote meetings, the following considerations must be observed by staff, pupils and parents:

- The meeting ID is to remain confidential and not to be shared to anyone that it was not designated to.
- Participants should join early to check technical equipment is working (camera and microphone).
- Participants are expected to have their cameras on to ensure validation of participant and safeguarding expectations are met.
- Participants should mute their microphone when not talking to limit distraction of background noise.
- A virtual hand should be raised should participants wish to make the meeting host aware of a contribution to discussion.
- Participants are expected to stay seated and stay present, avoiding doing background tasks (other screen work) or added distraction (shuffling papers, eating) so that all participants feel valued and respected.
- Recording, photos or screenshots of the meeting are not allowed by participants.

- The meeting may be recorded by the hosting teacher and stored in line with the school GDPR policy – participants will be notified in advance in these instances

The Internet

- Viewing, retrieving, downloading or transmitting illegal or inappropriate material is prohibited, as is knowingly visiting the 'dark web' or websites where such material may be found. Any pupils or staff discovering such sites must report the details to their teacher or line manager immediately.
- Intellectual property rights must be respected at all times. Pupils and staff must not create and/or transmit material which infringes copyright. It is plagiarism to pass off another's work as one's own and this extends to information obtained electronically. All internet sources must be acknowledged when producing pieces of work.
- Use of the school's internet and ICT facilities for financial gain, advertising or other commercial activities outside of those specifically approved by the School Leadership Team is prohibited.

ICT Hardware

- Pupils and staff must respect the School's network infrastructure and ICT equipment, and take appropriate care when using it. Any loss or damage, however caused, must be reported immediately to a relevant member of staff. Hardware must not be connected, disconnected or tampered with in any manner without explicit permission. Unnecessary waste or abuse of ICT resources (for example inappropriate printing) may result in financial charges and/or suspension of network access.

Artificial Intelligence (AI)

The school recognises that AI technologies are becoming part of modern education and society. The school is committed to ensuring AI is used safely, ethically and responsibility to enhance education while protecting children, staff and the wider school community.

- Human professional judgement must always take priority over AI-generated content. AI can support, not replace, the role of teachers and school staff.
- Staff may use AI tools to support professional tasks, however all AI-generated materials must be reviewed before use and checked for accuracy and bias.
- Staff should be aware of the risks of using AI tools whilst they are still being developed. Staff are not permitted to use AI with pupils without express permission from a senior leader. Should a decision be made to use it, a risk assessment will be carried out.
- Staff must not use AI to upload personal or confidential data or to make safeguarding decisions. Any suspected data breaches must be reported to the Headteacher/Data Protection Officer immediately.
- The school will risk assess AI tools before use with pupils, ensure filtering and monitoring systems are effective and teach pupils about misinformation and bias.
- The school will respond promptly to misuse or harmful content, in-line with Keeping Children Safe in Education (KCSIE) and the school Safeguarding Policy.

Cyberbullying and By Standers

- The school will not tolerate cyberbullying. Cyberbullying is defined as the use of information and communications technology (ICT), particularly e-mail, mobile phones and the internet, to deliberately upset someone else. It can take many forms, including threats, intimidation, harassment or cyberstalking by, for example, repeatedly sending unwanted messages or texts. Cyberbullying and the school's approach to this is referred to in the School's Behaviour and Bullying Policy.
- In cases of cyberbullying bystanders, or 'accessories' to the bullying, often have a more active role, e.g. forwarding messages or contributing to chat room discussions. Therefore although they may not have started the bullying they are active participants and often make the matter worse.
- The school makes it clear to all pupils that bystanders have a key responsibility to the school community and to anyone they see being bullied or victimised. They are encouraged not to tolerate such behaviour and to stand up for what they know to be right, for example by telling a member of staff what they have seen or heard. Access to the school's ICT resources is a privilege and continuance of this facility requires pupils to behave appropriately and to display a responsible attitude at all times.

The Use of Social Media

Professional Use of Social Media

Staff may use social media for professional, school related purposes in compliance with this policy.

Personal Use of Social Media

The school does not intend to unduly restrict its staff members' use of social media in their personal lives. However where a staff member makes identifiable personal use of social media, this can have a significant impact on the reputation and other interests of the Federation, directly or indirectly. Accordingly, staff members who engage in identifiable personal use of social media must minimise the risk of damage to our schools.

Staff members are personally responsible for use of social media in a personal capacity, including for the content they publish. Staff are not permitted to 'friend' or connect with pupils or ex-pupils of the school under the age of 18 years old using social media.

Rules for Use of Social Media

Staff should not upload any images of pupils in their personal communications and any use of images for professional use but be through the school platforms with the explicit consent of the pupils parents/carers along with the Headteacher of the school.

In professional use and identifiable personal use of social media, staff must:

- Only disclose and discuss publicly available information.
- Ensure that all content published is accurate and not misleading.
- Ensure that all content published complies with all relevant policies of the school.

- Expressly state on all postings that the stated views are their own and are not those of the school.
- Be professional in nature.
- Adhere to the Terms of Use of the relevant social media platform/website.
- Comply with the laws of copyright, privacy, defamation, contempt of court, discrimination and harassment, and all other applicable laws.

When accessing social media via the school's Internet, intranet and extranet systems, staff members must do so in a manner that is reasonable, responsible, ethical and lawful.

Specific Prohibitions

In professional use and identifiable personal use of social media, staff must not:

- Make any comment or post material that is, or might be construed to be, offensive, obscene, defamatory, discriminatory, hateful, racist or sexist towards any person.
- Make any comment or post material that creates, or might be construed to create, a risk to the health and safety of a staff member, contractor, student or other person, including material that amounts to "unacceptable behaviour" such as bullying, psychological or emotional violence, coercion, harassment, aggressive or abusive comments or behaviour, and/or unreasonable demands or undue pressure.
- Make any comment or post material that infringes copyright, is fraudulent, breaches intellectual property rights, constitutes a contempt of court, constitutes stalking, breaches a Court suppression order, or is otherwise unlawful.
- Imply that they are authorised to speak as a representative of the school, nor give the impression that the views they express are those of the school (unless they are officially authorised by the school Headteacher/Executive Headteacher).
- Use the identity or likeness of another employee, contractor, student or other stakeholder of the school.
- Use or disclose any confidential information obtained in their capacity as an employee or contractor of the school.
- Make any comment or post material that might otherwise cause damage to the school's reputation or bring it into disrepute.
- Use profane or offensive language or content.
- Include sexually explicit or pornographic content or links to sexually explicit or pornographic content.
- Include information that may tend to compromise the safety or security of the public or public systems.
- Include solicitations of commerce.
- Use the school or Viridis logo unless prior approval from the Headteacher/Executive Headteacher has been obtained.

Breach

Depending on the circumstances, non-compliance with this procedure may constitute a breach of employment or contractual obligations, misconduct, sexual harassment, discrimination, or some other contravention of policy, procedure or the law. Those who fail to comply with this procedure may face disciplinary action and, in serious cases, termination of their employment or engagement.

If a staff member notices inappropriate or unlawful content online relating to our schools, or content that may otherwise have been published in breach of this procedure, the staff member should report that content via email to ithelp@vs.hackney.sch.uk

Breaches of privacy, equal opportunity or other school procedures should also be reported in accordance with those procedures.

If directed by the School, a staff member must remove, and cooperate with all attempts to remove, any comment, post or other online content that the School deems to be in breach of this procedure or any other School procedure.

Technical and Infrastructure Approaches

The school:

- Has an educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL 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' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of pupils.
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were 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.
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- Uses security time-outs on Internet access where practicable / useful.
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with students as this has email content control and the address does not identify the student or school.
- Provides staff with an email account for their professional use, 365, and makes clear personal email should be through a separate account.
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies.

Education and training

The school:

- Fosters a 'no blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident.
- Ensures all pupils know how to report any abuse.
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes training available annually to staff.
- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site
  - demonstrations, practical sessions held at school
  - distribution of 'think u know' for parents materials
  - suggestions for safe Internet use at home
  - provision of information about national support sites for parents

Links to other policies

- Behaviour & Bullying Policy
- Safeguarding Policy
- Parent Partnership Policy
- Learning & Teaching Policy
- Data Protection Policy
- Charging and Remissions Policy
- CCTV Policy

Appendix A

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.

A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites / bookmarks are a useful way to present this choice to pupils.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk.

Images usually have copyright attached to them and this is a key teaching point to pupils and staff.

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE.

Webcams and Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project. Video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom. For large group work high quality video conferencing hardware equipment is required to be plugged into the

network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2. Advice can be found here http://www.lgfl.net/SERVICES/CURRICULUM/Pages/WeatherStations.aspx http://www.lgfl.net/learningresources/VideoConferencing/Pages/Home.aspx

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

Social Networking Sites
These are a popular aspect of the web for young people. Sites such as Facebook, My Space, Habbo Hotel, Bebo, Piczo, and YouTube allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children and adults. They are environments that should be used with caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. [See Education programme]

Our schools will generally block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school..

Podcasts
Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area.
http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Chatrooms
Many sites allow for ‘real-time’ online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms.

Appendix B

Rules for Pupils

Keeping safe: stop, think, before you click! Rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will not look at other people's files without their permission and I will only delete my own files.
- I will keep my login and password secret.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved. The emails and messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult and where I can, I will save or print a copy of the message to show to a teacher/ responsible adult.
- I will tell an adult if I see something on the internet that upsets or worries me e.g. images of people of being unkind.

Appendix C

Safer Internet Use. Key Curriculum Content.

Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion
- to develop a range of strategies to validate and verify information before accepting its accuracy
- to skim and scan information
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand why and how some people will 'groom' young people for inappropriate or dangerous reasons