PATRON
HM THE QUEEN

LVS Ascot
A Co-educational Day & Boarding School
for young people aged 4 - 18

ONLINE SAFETY POLICY

Whole school including the EYFS

Relevant Statutory Regulations:	ISSR Part 1 Para 3(f). Part 3 Para 7. NMS 8, 9. General Data Protection Regulation 2018. Keeping Children Safe in Education 2024
Nominated member of SMT responsible for the policy:	Laura Collins
Updated:	01 September 2024
Date of next review:	01 September 2025

Contents

INTRODUCTION

- This online safety policy has been written by LVS Ascot (hereafter referred to as 'school'), involving staff, pupils and parents/guardians.
- It takes into account the DfES statutory guidance Keeping Children Safe in Education 2024.
- The policy focuses on the role of online safety in the school setting, supported via technology supplied, monitored and maintained by the LTC IT Team (TSC). The LTC is responsible for online safety elsewhere in the charity, including the monitoring of staff.

- The purpose of this online safety policy is to:
  - Safeguard and protect all members of the school community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Require all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- The school broadly categorises online safety issue into four areas of risk, in line with KCSIE 2024:
  - Content: exposure to illegal, inappropriate or harmful material
  - Contact: subjection to harmful online interaction with other users
  - Conduct: an increase in the likelihood of harm through online behaviour
  - Commerce: introduction to gambling through websites

Policy Scope

- The school
  - Recognises online safety as an essential part of safeguarding and acknowledges its duty to protect all pupils and staff from potential harm online.
  - Identifies the internet and personal and school devices (e.g., computers, tablets, mobile phones and games consoles) are an important part of everyday life.
  - Believes pupils should be empowered to build resilience, be educated and develop strategies to manage and respond to risk online.
- This policy applies to all staff including the Trustees and governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (hereafter collectively referred to as "staff") as well as pupils, parents and guardians.
- This policy applies to all internet access and use of technology, including personal devices, or where pupils, staff or other individuals are provided with

school-issued devices for use off-site, such as a work laptops, tablets or mobile phones.

LINKS WITH OTHER POLICIES AND PRACTICES

This policy links with several other policies including:

- Anti-bullying Policy
- Code of Conduct
- Personal Conduct Policy
- Safeguarding Policy
- Curriculum Policy
- Photography Policy
- Pupil Personal Digital Devices Policy
- Social Media Policy

MONITORING AND REVIEW

- As technology evolves rapidly, this policy requires at least annual review.
  - Additionally, the policy requires revision following any national or local policy requirements, any safeguarding concerns or any changes to the technical infrastructure.
- The school monitors internet use and evaluates online safety mechanisms to ensure this policy consistently applied.
- To ensure oversight of online safety, the Principal is informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into school action planning.

ROLES AND RESPONSIBILITIES

- The Designated Safeguarding Lead ('DSL') has responsibility for online safety.
- The school recognises all members of the community have important roles and responsibilities with regard to online safety.

The Senior Management Team through the LTC IT Department (TSC) will:

- Ensure online safety is a safeguarding issue and practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety - including a staff code of conduct/personal conduct policy/social media and/or acceptable use policy ('AUP')
- Ensure suitable and appropriate filtering and monitoring systems are in

place and work with technical staff to monitor the safety and security of school systems and networks.

- Embed online safety within a progressive curriculum enabling all pupils to develop an age-appropriate understanding of online safety through LifeLearning lessons and other means of dissemination.
- Support the DSL by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Undertake appropriate risk assessments regarding the safe useof technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure staff are aware of their responsibilities to effectively monitor usage of the devices and content through both WiFi and 4G and 5G networks

The Designated Safeguarding Lead (DSL) will:

- Act as the named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside the Safeguarding Team to ensure online safety is recognised as part of the school's safeguarding responsibilities and implement a coordinated approach.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training, using both online and face-to-face training methods.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant, up to date knowledge to keep pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks pupils with Special Educational Needs and Disabilities (hereafter 'SEND') face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, e.g., National Online Safety Day.
- Promote online safety to parents, guardians and the wider community through a variety of channels and approaches including LVS Perspectives, National Online Safety platform
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms through CPOMs
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the SMT and governing body.
- Work with the SMT to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the governor with a lead responsibility for safeguarding and/or online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the code of conduct, social media policy, online safety policy and AUPs.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Monitor student usage of the internet through school and or personal devices when used in lessons.

It is the responsibility of the LTC IT (TSC) staff managing the technical environment to:

- Provide technical support and perspective to the DSL and SMT, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures such as use of passwords and encryption to ensure the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Apply and update the school's filtering policy on a regular basis; responsibility for its implementation is shared with the SMT.
- Reporting any safeguarding concerns, identified through monitoring or filtering breaches, to the DSL in accordance with the safeguarding procedures.
- Ensure that the filtering and monitoring systems and procedures in place are effective.

It is the responsibility of pupils (at a level appropriate to their individual age and ability) to:

- Read, sign and adhere to the AUPs and Personal conduct.
- Read and understand the School's mobile phone and online safety policy.
- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others who may be experiencing online safety issues.

It is the responsibility of parents and guardians to:

- Read and sign the AUPs and encourage their children to adhere to them.
- Read and understand the School's Online Safety, Social Media, Personal Conduct and Mobile Phone policy.
- Support school online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Model safe and appropriate use of technology.
- Identify changes in behaviour could indicate their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters risk or concerns online.
- Contribute to the development of the online safety policies.
- Use school systems, such as learning platforms and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

EDUCATION AND ENGAGEMENT APPROACHES

Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in the Life Learning Programme.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
  - Provide drop down days or specific lectures on online safety for all age children.
- The school will support pupils to read and understand the AUPs in a way which suits their age and ability by:
  - Informing pupils that network and internet use is monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking pupil voice when developing online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors where appropriate, to complement and support school internal online safety education approaches.

Vulnerable Pupils

- The school recognises some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with SEND or mental health needs, those perceived to be LGBTQ+ , children with English as an Additional Language (EAL) and children experiencing trauma or loss.
- The school provides differentiated and ability-appropriate online safety education, access and support to vulnerable pupils.
- When implementing an appropriate online safety policy and curriculum, the school will seek input from specialist staff as appropriate.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis – with at least annual updates – as part of existing safeguarding and child protection training/updates.
    - This covers the potential risks posed to pupils (Content, Contact and Conduct, Commerce) as well as the school's professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that the school monitors its IT systems and can trace activity to individual users; staff will be reminded to behave professionally and in accordance with school policies when accessing school systems and devices.
- Make sure staff are aware that all devices' internet activity is decrypted and subject to internet filtering in accordance with the LTC BYOD Policy.
- Make staff aware their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation through the Staff Code of Conduct
- Highlight useful educational resources and tools staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

Awareness and engagement with parents and guardians

- The school recognises parents and guardians have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and guardians by:
    - Providing information and guidance on online safety in a variety of formats.
        - This includes offering specific online safety awareness training and highlighting online safety at other events, e.g., parent evenings and transition events.
    - Drawing attention to the online safety policy and expectations, e.g., via newsletters, letters, broadcasts etc.
    - Requesting they read online safety information when joining the school community as part of the home-school agreement.
    - Requiring them to read the school's AUPs and discussing the implications with their children.
    - Providing all parents and carers with a National Online Safety login and password for parents to engage with support and training

REDUCING ONLINE RISKS

- The school recognises the internet is a constantly evolving environment and due to its global and connected nature, it is not possible toguarantee unsuitable material cannot be accessed via the school computers or devices.
- To minimise exposure to unsuitable material, the school will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before permitting use in school.
    - Ensure appropriate filtering and monitoring is in place and taking all reasonable precautions to ensure users can access only appropriate material.
- All members of the community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos that could cause harm, distress or offence to members of the community. The school's AUPs outline these expectations which are further highlighted through a variety of education and training approaches.

SAFER USE OF TECHNOLOGY

Classroom Use

- The school uses a wide range of technology, including (but not limited to) access to
    - Computers, laptops and other digital devices
    - Internet (including search engines and educational websites)
    - Email
    - Digital cameras, web cams and video cameras

    - Microsoft Teams
- All school-owned devices will be used in accordance with the AUPs and with appropriate safety and security measures in place.
- Members of staff evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of the school community.
- The school will ensure the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Managing Internet Access

- The school will maintain a written record of users granted access to school devices and systems.
- All staff, pupils and visitors will read and sign an AUP before granted access to the school computer system, IT resources or internet.

FILTERING AND MONITORING

Decision Making

- The school ensures age and ability appropriate filtering and monitoring are in place to limit pupils' exposure to online risks.
- The school is aware of preventing "over blocking" which may unreasonably restrict what can be taught.
- Decisions regarding filtering and monitoring are risk assessed considering the school's specific needs and circumstances.
- Changes to filtering and monitoring are risk assessed by staff with educational and technical experience and with consent from the leadership team.
- The SMT performs regular checks to ensure both filtering and monitoring are effective and appropriate.
- All members of staff understand filtering and monitoring alone cannot fully safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- The school currently uses Smoothwall
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- If pupils discover unsuitable sites:
    - They are required to turn off monitor/screen and report the concern to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or technical staff.
    - The breach is recorded and escalated.
    - Parents/guardians are informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies.

Monitoring (to be amended upon implementation of SENSO)

- The school monitors internet use on all school-owned or provided internet- enabled devices. This is achieved by:
  - Physical monitoring (supervision),
  - Internet monitoring and filtering
- If monitoring identifies a concern, the school will respond accordingly.
- All users will be informed that use of the school system is monitored in line with data protection, human rights and privacy legislation.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available in accordance with General Data Protection Regulations and Data Protection legislation.

SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS

- The school take appropriate steps to ensure the security of school information systems, including:
  - Regular updates to virus protection.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media is checked by anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on the school network,
  - The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords are enforced for all members of the school community.
  - All users must log off or lock their screens/devices if systems are unattended.

Password policy

- All members of staff will have their own unique username and private passwords to access the school systems; members of staff are responsible for keeping their password private.
- All pupils have their own unique username and private passwords to access the school systems; pupils are responsible for keeping their password private.
- The school require all users to:
  - Use strong passwords to access the school system.
  - Change their passwords when prompted.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

Managing the Safety of the School Website

- The school ensures information posted on the website meets the requirements identified by the Department for Education (DfES).
- The school will ensure the website complies with guidelines for publications including accessibility, data protection, and respect for intellectual property rights, privacy policies and copyright.
- Staff or pupil’s personal information is not published on the school website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Publishing Images and Videos Online

- The school will ensure all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

- Access to school email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, AUPs and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication containing sensitive or personal information will only be sent using secure and encrypted email.
  - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform the LTC IT Department (TSC) desk if they receive offensive communication and this will be recorded

in the school safeguarding files/records.

- Excessive social email use can interfere with teaching and learning and will be restricted.

Staff email

- The use of personal email addresses by staff for any official school business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.
- All members of staff are required to read, sign and adhere to the appropriate AUP.

Pupil email

- Pupils will use provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

MANAGEMENT OF APPLICATIONS (APPS) USED TO RECORD CHILDREN'S PROGRESS

- The school uses iSAMS to track pupils' progress and share appropriate information with parents and guardians.

- The school uses CPOMs to record any concerns relating to pupils including behaviour, online safety, safeguarding and child protection concerns.

- The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure the use of tracking systems is appropriately risk assessed prior to use and used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard pupils' data:
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps that record and store pupils' personal details, attainment or images – including Outlook.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and guardians will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

use, along with expectations for safe use and action taken to safeguard the community.

  - Only social media tools that have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving pupils will be moderated possible.
- Parents and guardians will be informed of any official social media use with pupils; written parental consent will be obtained, as required.
- The school will ensure any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

USE OF PERSONAL DEVICES AND MOBILE PHONES

- The school recognises personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/guardians, but technologies must be used safely and appropriately within the school.

- For further information, refer to the Personal Digital Devices Policy.

Expectations

- All use of personal devices (e.g., tablets, games consoles and 'smart' watches and mobile phones) will take place in accordance with the law and other appropriate policies.
- Electronic devices of any kind brought onto site are the responsibility of the user.
  - All members of the school community must to take steps to protect their personal devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on the school premises.
  - All members of the school community are advised to use passwords/PINs to ensure unauthorised calls or actions cannot be made on their phones or devices. Passwords and PINs should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones are banned whilst on school site, or under the jurisdiction of the school except on
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- Sending abusive or inappropriate messages or content via personal devices by any member of the community is forbidden. Breaches will be dealt with as part of the school behaviour policy.
- All members of the school community are advised to ensure their personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene school behaviour or child protection policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure use of personal devices takes place in accordance with the law, as well as relevant policies and procedures, such as confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
  - Keep personal devices in a safe and secure place during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, unless the Principal has given written permission, such as in emergency circumstances.
  - Ensure any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
  - Ensure privacy by closing any open windows on personal devices before connecting – manually or automatically – the device to the school internet system.
- Members of staff may not use their own personal devices to contact

pupils or parents and guardians.

  - Any pre-existing relationships that could undermine this will be discussed with the DSL.
- Staff will not use personal devices:
  - To take photos or videos of pupils and will only use school-provided equipment for this purpose.
  - Directly with pupils and will only use work-provided equipment during lessons or educational activities.
  - During lessons or in the dining hall at mealtimes.
- If a member of staff breaches the school policy, action will be taken in line with the appropriate school policy.
  - If a member of staff is thought to have illegal content saved or stored on a personal device or have committed a criminal offence, the Police will be contacted.

Pupils' Use of Personal Devices (please refer to the mobile phone policy)

- Pupils will be educated regarding the safe and appropriate use of personal devices and made aware of boundaries and consequences.
- Only tablets, surface pros or laptops may be used for educational purposes in school and lesson times.
- Gaming is not permitted at any time, during lessons or recreational times.
- If a pupil needs to contact his/her parents or guardians they will be allowed to use a school phone or their personal device in the Student Reception only.
  - Parents are advised to contact their child via the school office.
- Personal devices must not be taken into examinations.
  - Pupils found in possession of a mobile phone, smart watch or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from that or all examinations.

Visitors' Use of Personal Devices and Mobile Phones

- Parents/guardians and visitors (including volunteers and contractors) must use their personal devices in accordance with the school's AUP and other associated policies.
- The school will ensure appropriate signage and information is displayed and provided to inform parents, guardians and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL or SMT of any breaches of the school policy.

Officially provided mobile phones and devices

- Certain members of staff will be issued with a work phone number and email address, where contact with pupils or parents/guardians is required.
- School mobile phones and devices will be protected via a passcode/password/PIN and must only be accessed or used by members of

staff.

- School mobile phones and devices will be used in accordance with the AUP and other relevant policies.

RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (), cyberbullying and illegal content.

Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns through CPOMs and or other means of direct reporting.
- The DSL will record these issues in line with the school's safeguarding policy.
- The DSL will ensure online safety concerns are escalated and reported to relevant agencies.
- The school will inform parents and guardians of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse should be made following the guidance outlined in the Whistleblowing Policy and/or Low Level Concerns policy
- Appropriate action will be taken in accordance with the LTC Code of Conduct for Employees.

PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

All online safety incidents or concerns must be reported immediately to the DSL in line with the Safeguarding policy and KCSIE 2024, these include but are not limited to:

- YPSI (Youth Produced Sexual Imagery)
- Online Hate – and potential radicalization
- Online bullying incidents
- Gambling
- Gaming,
- Sexual Harassment and sexual abuse.
- Indecent Images of Children