E-SAFETY POLICY

Whole school including the EYFS

Relevant Statutory Regulations:	ISSR Part 1 Para 3(f). Part 3 Para 7. NMS 11. General Data Protection Regulation 2018. Keeping Children Safe in Education 2019.
Nominated member of SMT responsible for the policy:	Bryan Padrick
Updated:	01 October 2021
Date of next review:	01 October 2022

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 2021.
- The policy focuses on the role of e-safety in the school setting, supported via technology supplied, monitored and maintained by the LTC IT Team (TCS). The LTC is responsible for e-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 three areas of risk:
    - 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

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 associated 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 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
- Acceptable Use Policies (AUPs)
- Code of Conduct/Staff Behaviour Policy
- Behaviour Policy
- Safeguarding Policy
- Curriculum Policy,
- Photography Policy
- 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 lead 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/behaviour policy and/or acceptable use policy ('AUP') - covering acceptable use of technology.
- 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.
- 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 use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

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.
- 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., Safer Internet Day.
- Promote online safety to parents, guardians and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- 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 half-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 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.

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.

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

- Read, sign and adhere to the AUPs.
- 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.
- 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 LV4Life 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.
- The school will support pupils to read and understand the AUPs in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - 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, 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) 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.
- 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, 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.

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 to guarantee 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
- 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 use Impero to alert access to and block prohibited sites categorised.
- 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

- 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 use WCBS/PASS/3SYS to track pupils' progress and share appropriate information with parents and guardians.

- 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.

SOCIAL MEDIA

Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the school community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of the school community must engage with social media in a positive, safe and responsible manner.
    - All members of the school community are advised to not publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school-provided devices and systems on site.
    - The use of social media between 08:40 – 16:00 for personal use is not permitted.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the school community on social media should be reported to the DSL and managed in accordance with the appropriate policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction. This will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school code of conduct/behaviour policy and as part of the AUPs.
- All members of staff are advised their online conduct on social media can have an impact on their role and reputation within the school.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include

(but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as the school's.

- Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.
- All members of staff are encouraged to consider the information, including text and images, they share and post online and to ensure their social media use is compatible with their professional role and is in accordance the school policies and the wider professional and legal framework.
- Information and content staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the SMT immediately if they consider any content shared on social media sites conflicts with their role.

Communicating with pupils and parents and guardians

- Members of staff should not communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this should be discussed with the DSL.
  - If contact with pupils is required once they have left the school, members of staff are expected to use existing alumni networks or official school-provided communication tools.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstances whereby the Principal has given prior approval.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media is taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- The school are aware many popular social media sites state they are not for

children under the age of 13; therefore, the school will not create accounts specifically for pupils under this age.

- Any concerns regarding pupils' use of social media are addressed in accordance with existing policies.
    - Concerns are shared with parents/guardians as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the school and externally.

Official Use of Social Media

- The school official social media channels are:
    - *Twitter, Facebook, LinkedIn and YouTube channel.*
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Principal.
    - SMT have access to account information and login details for the school social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official social media channels.
    - Official social media sites protected and, where possible, linked to the school website.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use is conducted in line with existing policies.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/guardians and pupils will be informed of any official social media

use, alongwith 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 ofthe community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacityas an employee of the school, they will:
    - Always be professional and aware they are an ambassador for the school.
    - Disclose their official role and/or position but make it clear they do not necessarily speak on behalf of the school.
    - Always be responsible, credible, fair and honest, and consider how the information published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and guardians.
    - Inform their line manager, the DSL and/or the Principal of any concerns, such as criticism, inappropriate content or contact from pupils.

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 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.
- 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 and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and made aware of boundaries and consequences.
- The school expects pupils' personal devices to be used appropriately within school and not in lessons.
- 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.
    - Parents are advised to contact their child via the school office.
- Personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal devices for a specific education purpose does not mean blanket use is permitted.
- Personal devices must not be taken into examinations.
    - Pupils found in possession of a mobile phone 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.
- If a pupil breaches the policy, the phone or device will be confiscated and held in a secure place.
    - Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will only be carried out in accordance with the school policy. www.gov.uk/government/publications/searching-screening-and-confiscation)
    - A member of the SMT, with the consent of the pupil or a parent/carer, may search pupils' mobile phones or devices. Content may be deleted or

requested to be deleted, if it contravenes the school policies. (www.gov.uk/government/publications/searching-screening-and-confiscation)

- Mobile phones and devices have been confiscated will be released to students at the end of the day
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the Police for further investigation.

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

- 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 (sexting), cyberbullying and illegal content.

Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- 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.
- Appropriate action will be taken in accordance with the LTC Code of Conduct for Employees.

PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

Online Sexual Violence and Sexual Harassment between Children

- The school has accessed and understood *Sexual violence and sexual harassment between children in schools and colleges* (2018) guidance and Part 5 of Keeping Children Safe in Education 2019.
- The school recognises sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how the school will respond to concerns relating to sexual violence and sexual harassment between children is in the school's safeguarding policy and anti-bullying policy.
- The school recognises the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The school will ensure all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability-appropriate educational methods as part of the PSHE and RSE curriculum
- The school will ensure all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- The school will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on school premises or using school equipment.
- If made aware of online sexual violence and sexual harassment, the school will:
    - Immediately notify the DSL in accordance with the school child protection and anti-bullying policies.

- If content is contained on pupils' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with school policy.
- Inform parents and guardians, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Bracknell Forest Safeguarding Partnership.
- If the concern involves children and young people at different schools, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL will discuss this with the Police first to ensure investigations are not compromised.
- Review the handling of any incidents to ensure best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to the DSL.
- The school will ensure all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability-appropriate educational methods.
- The school will ensure all members of the community are aware of sources of support regarding youth produced sexual imagery.
- The school will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using school provided or personal equipment.
- The school will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If deemed necessary, the image will only be viewed by the DSL and justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (e.g., youth produced sexual imagery) and will not allow or request pupils to do so.
- If made aware of an incident involving the creation or distribution of youth

produced sexual imagery, the school will:

- Act in accordance with the school's safeguarding policy and the Bracknell Forest Safeguarding Partnership procedures.
- Ensure the DSL responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance (UKCCIS, August 2016).
- Store the device securely.
    - If an indecent image has been taken or shared on the school network or devices, the school will act to block access to all users and isolate the image.
- Carry out a risk assessment that considers any vulnerability of pupils involved, including carrying out relevant checks with other agencies.
- Inform parents and guardians, if appropriate, about the incident and how it is being managed.
- Make a referral to Bracknell Forest Safeguarding Partnership and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with school policy, taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS, August 2016 guidance.
    - Images will only be deleted once the DSL has confirmed other agencies do not need to be involved; and are sure to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure best practice was implemented; the SMT will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The school will ensure all members of the community are aware of online child sexual abuse, including exploitation and grooming, the consequences and possible approaches that may be employed by offenders to target children and how to respond to concerns.
- The school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- The school will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/guardians.
- The school will ensure all members of the community are aware of the support available regarding online child sexual abuse and exploitation

(including criminal exploitation), both locally and nationally.

- The school will ensure the 'Click CEOP' report button is visible and available to pupils and other members of the school community via LVSpace.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), the school will:
    - Act in accordance with the school safeguarding policy and the relevant Bracknell Forest Safeguarding Partnership procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to the Bracknell Forest Safeguarding Partnership (if required/ appropriate) and immediately inform the Police.
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/guardians about the incident if appropriate and how it is being managed.
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure best practice is implemented. The SMT will review and update any management procedures, where necessary.
- The school will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on the school premises or using school provided or personal equipment.
    - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre
- If the school are unclear whether a criminal offence has been committed, the DSL will immediately obtain advice through the Police.
- If pupils at other school are believed to have been targeted, the DSL will seek support from the Police and/or the Bracknell Forest Safeguarding Partnership first to ensure potential investigations are not compromised.

Indecent Images of Children (IIOC)

- The school will ensure all members of the community are aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will respond to concerns regarding IIOC on the school equipment and/or personal equipment, even if access took place off-site.
- The school will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If the school are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Police and/or the Bracknell Forest Safeguarding Partnership.
- If made aware of IIOC, the school will:
    - Act in accordance with the school's safeguarding policy and the relevant Bracknell Forest Safeguarding Partnership's procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Thames Valley Police or the LADO (if involving staff).
- If made aware a member of staff or a pupil has been inadvertently exposed to indecent images of children, the school will:
    - Ensure the DSL is informed.
    - Ensure the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and guardians.
- If made aware indecent images of children have been found on the school-provided devices, the school will:
    - Ensure the DSL is informed.
    - Ensure the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure any copies that exist of the image, for example in emails, are deleted.
    - Inform the Police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) if requested by the Police.
    - Report concerns, as appropriate, to parents and guardians.
- If made aware a member of staff is in possession of indecent images of children on school-provided devices, the school will:
    - Ensure the Principal is informed in line with school policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school policy.
    - Quarantine any devices until Police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at the school.
- Full details of how the school will respond to cyberbullying are set out in the school's anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at the school and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordancewith relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Bracknell Forest Safeguarding Partnership.

ONLINE RADICALISATION AND EXTREMISM

- The school will take all reasonable precautions to ensure pupils and staff are safe from terrorist and extremist material when accessing the internet on site.
- If the school are concerned a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the school's safeguarding policy.
- If the school are concerned a member of staff may be at risk of radicalisation online, the Principal will be informed immediately, and the safeguarding policy actioned.