Villa Real School

together we achieve

Online Safety Policy 2025

Responsibility: Alan Granton Date: October 2025

Signed & Adopted by the Governing Body:

Chair of Governors

Date: 18.11.25

To be reviewed: October 2026

Legal and Policy Framework

This policy should be read alongside and implements the expectations in:

Keeping Children Safe in Education (KCSIE) 2025 (statutory) – leadership, filtering/monitoring, training, reporting and DSL role.

DfE Filtering & Monitoring Standards – annual review, defined roles, proportionate filtering, effective monitoring.

Teaching online safety in schools – curriculum embedding and whole-school approach.

UKCIS – Education for a Connected World (2020) – age-appropriate learning outcomes across eight strands.

Prevent Duty guidance (2023) – risk assessment, training, reducing permissive environments, visiting speaker controls.

DfE Cyber Security Standards – risk assessment, access control, incident response, backups.

ICO & DfE data protection guidance – lawful bases, privacy information, images and videos of pupils (UK GDPR).

The Online Safety Act 2023

<u>Villa Real School Policy & Legislation</u>

Villa Real School Anti-Bullying Policy 2024
Villa Real School ICT Policy 2024
Villa Real School PSHCE Policy 2024

AIMS AND SCOPE

In today's society children, young people and adults interact with technologies such as mobile phones, tablets, games consoles, SMART phones and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but may occasionally place children, young people and adults in danger.

Online safety is an essential element of education and educational settings This Online Safety Policy sets out strategic guidelines, procedures and protocols ensuring all members of the School community are equipped with the skills and knowledge to make safe and responsible decisions, are following protocols and guidelines within the law and legislation, are aware of professional conduct, prepared in managing risks, and feel able to report any concerns.

This Online Safety Policy sets out guidelines and protocols for the whole school community ensuring safe use of the internet, mobile phones, tablets and any other electronic communication devices; both in and out of school settings.

Set out in this policy is guidance for all staff and the importance of good online safety practice in order to protect and educate the pupils/students in their care. Members of staff are strategically informed about how to manage their own professional reputation online and actively demonstrate appropriate online behaviours compatible with their role in the School Community.

- Villa Real School's Online Safety Policy has been written by the School, involving staff, pupils/students and parents/carers, building on the DCC Online Safety Policy template with specialist advice and input as and where required
- This Policy has been approved by Villa Real School's Senior Management Team and adopted by the Governing Body indicated by date of adoption on front of policy
- The School has an appointed Governor responsible for lead in online safety
- The Online Safety Policy will be reviewed annually or sooner if required

Responsibilities/ Roles

The Designated Safeguarding Lead: Jill Bowe
The Online Safety Lead for the Governing Body: Caroline Spence
The Online Safety Team Lead: Alan Granton
School Network Manager: Andrew Moore

STATEMENT

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

PURPOSE

- Clearly identify the key principles expected from all members of the School community with regards to the safe and responsible use of technology, ensuring that Villa Real School is a safe and secure environment
- Raise awareness with all members of Villa Real School regarding the potential risks and benefits of technology
- To enable all members of staff to work safely and responsibly, to role model positive behaviour online and have an awareness of the need to manage their own professional standards and practice when using technology
- Identify clear procedures and protocols when responding to online safety concerns that are known by all members of the School Community

This Online Safety Policy applies to all staff including the Governing Body, Teachers, Support staff, cleaning staff, kitchen staff, building and maintenance staff, external contractors, visitors, work placement students, teaching students, volunteers medical students and any other external agencies and persons, as well as parents/carers, pupils/ students and work place students.

Key Responsibilities of Villa Real School Management and Leadership Team

The Senior Management Team, including the Governing Body of Villa Real School, has statutory responsibilities for child protection, of which online safety is an essential element.

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with local recommendations with appropriate support and consultation throughout the School Community
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture
- Supporting the designated Safeguarding Lead by ensuring they have sufficient resources to fulfil their online roles and responsibilities
- Ensure there are appropriate and up to date policies and procedures regarding online safety including an acceptable use policy which covers appropriate professional conduct and use of technology
- To ensure that suitable and appropriate filtering systems are in place to protect pupils/ students from inappropriate content which meet the needs of the School community whilst ensuring pupils/ students have access to required educational material
- To work with and support technical staff in monitoring the safety and security of Villa Real School's systems and networks and to ensure that Villa Real School's network and systems are actively monitored
- Ensuring all members of staff receive regular, up to date, appropriate training regarding online safety roles and responsibilities and provide all with guidance regarding safe appropriate communications
- Ensuring that online safety is embedded within a progressive curriculum which enables all pupils/students to develop an understanding of online safety and the associated risks and safe behaviours
- To be aware of any online safety incidents and ensure that; where appropriate the external agencies and support are sought and liaised with accordingly
- Receiving and regularly reviewing online safeguarding records and using these to inform and shape future practice
- Ensuring robust reporting channels and systems are implemented and easily accessible for the Villa Real School Community to report any safety concerns; this including internal, local and national support
- Ensure appropriate risk assessments are undertaken regarding the safe use of technology, including the safe and responsible use of devices
- To ensure a member of the Governing body is identified with a lead responsibility for supporting online safety

The Key Responsibilities of the Online Safety Lead

- Working with DSL (Designated Safeguarding Lead) ensuring all safeguarding incidents -online or otherwise are dealt with accordingly following the School's safeguarding procedures
- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate

- Keeping up to date with current research, legislation and trends regarding online safety
- Co-ordinating participation in local and national events to promote positive online behaviour
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- Work with Villa Real School lead for data protection and data security to ensure practice is in line with current legislation
- Maintaining a record of online safety/ incidents and concerns including actions taken as part of Villa Real School's safeguarding recording mechanisms
- Monitor regularly Villa Real School's online safety incidents; identifying any gaps or trends, reflect and use the information/data to inform and update future responses
- Report to SMT (Senior Management Team) and where necessary and appropriate other agencies online safety concerns
- Liaise with DCC and external bodies where appropriate
- Work with Villa Real School's SMT to review and update online safety policies and procedures, AUP policies and any other related policies, legislation and guidelines
- Ensure online safety is integrated with other school policies and procedures
- Support/ lead online safety group

All members of Villa Real School have an essential role to play in ensuring the safety and wellbeing of others, both on and off line. It is important that all members of the School Community are aware of their roles and responsibilities and where necessary how to access and seek support and guidance.

The Key responsibilities for all members of staff are:

- Contributing to the development of online safety policies and safe practices within school setting and beyond
- Reading the School's Acceptable Use Policy/ guidelines and adhering to them
- Taking responsibility for the security of school systems, data and equipment
- Having an awareness of a range of different online safety issues and how they may relate to the pupils/students in their care
- Modelling good practice when using new, emerging and existing technologies and devices
- Embedding online safety within the educational curriculum delivery wherever possible
- Identifying individuals of concern and taking appropriate action by following school safeguarding policy and procedures

- Knowing when and how to escalate online safety issues, reporting systems both internally and externally
- Being able to signpost to appropriate support available for online safety issues both internally and externally
- Maintaining a professional acceptable level of conduct in their personal use of technology including social media usage, both on and off site
- Demonstrating an emphasis on positive learning opportunities
- Taking personal responsibility for professional development and conduct in this area
- Attending online safety training and if unable to do so contacting the online safety lead to update their skills and knowledge at an appropriate time.
- **To be read alongside Appendix A**

The Key Responsibilities for staff managing the technical environment
The responsibility for managing the technical environment is ultimately the responsibility of the Headteacher and Governing Body. Villa Real School make use of an internal network manager engineer, while also seeking assistance of the local authority as part of the school's service agreement.

The responsibility for managing these services rests with a member of staff from Villa Real School Senior Management Team.

The Headteacher and School Business Manager are responsible for managing any external technical service provider and help ensure the technical support in school has relevant appropriate resources to help ensure that the technical environment within school is both safe and secure.

In addition to the above, further key responsibilities are;
- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are maximised
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team
- To ensure suitable access controls and encryption is implemented to protect personal and sensitive information held on school owned systems and devices
- Ensuring that the use of Villa Real School's network is regularly monitored and reporting any deliberate or accidental misuse to the Designated Safeguarding Lead
- Report any breaches or concerns to the Designated Safeguarding Lead and Senior Management Team and together ensure that these breaches/ concerns are reported and recorded accurately with the appropriate action taken as advised

- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure
- Reporting any breaches and liaising with the local authority or other local and national bodies as appropriate on technical infrastructure issues
- Providing technical support and perspective to the Designated Safeguarding Lead and Senior Management Team, especially in the development and implementation of appropriate online safety procedures and policies
- Ensuring that the School's ICT infrastructure/systems are secure and not open to misuse or malicious attack
- Ensuring appropriate anti-virus software and systems are installed and maintained on all setting machines and devices- including portable devices
- Ensure that appropriate strong passwords are enforced for all staff
- Ensuring staff have the opportunity to read and understand the online safety policy.

Key Responsibilities of Pupils/ Students. To be read alongside Appendix A

At a level that is appropriate to their individual age, ability and vulnerabilities

- Contributing to the development of online safety policies
- Reading (if able or have read to) and adhering to Villa Real School's Acceptable Use Policy
- Respecting the feelings and rights of others both on and offline
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues
- Take responsibility for keeping themselves and others safe online
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit risks
- Use technology in a positive way to benefit themselves and others.
- Comply with current legislation

Key responsibilities of parents and carers are

- Reading Villa Real School's Acceptable Use Policy and encourage their children to adhere to them, and adhering to them themselves where appropriate
- Discussing online safety issues with their children and support the School in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- Role modelling safe and appropriate use of technology whilst online and off line and social media
- Identifying changes in behaviour that their child is at risk of harm online

- Seeking help and support from the School and or other appropriate agencies, if their child encounters online problems and or has any online concerns
- Contributing to the development of Villa Real School's Acceptable use policy
- Using school systems, such as learning platforms and other network resources safely and appropriately
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Supporting the School's policies with regards to the use of mobile technology.

Managing the Villa Real School Website
Schools are required to publish certain information online- this means schools *must* have a website. The most recent guidance reading information that must be published online can be found at https://www.gov.uk/what-maintained-schools-must-publish-online

Villa Real School will:

- Ensure that the information posted on the School website meets the requirements as identified by the Department for Education (DfE)
- The contact details of Villa Real School will be the address, email and telephone number. Staff or pupil's/student's personal information **will not** be published
- The Headteacher will take overall editorial responsibility for online content published and will ensure that all information is accurate, appropriate and up to date
- The School website will comply with the School's guidelines for publications including accessibility respect for intellectual property rights, privacy notices/ policies and copyright
- Email addresses will be published carefully online, to avoid being harvested for spam
- Pupils/students work will be published with their permission or that of their parents/ carers
- Pupils'/ student's images/ photographs will be published with the permission of their parents/ carers
- The administrator account for the School website will be safeguarded appropriately with a strong password- this password will not be shared with any unauthorised person/ persons
- The School will post information about safeguarding, including online safety, on the School website for members of the community

Publishing images and videos online
Still and moving images and sound add liveliness add interest to a publication, display or website particularly when pupils/ students are included. Never the less the safety and security of staff and pupils/ students is paramount. Images of a child must not be published without the parents/ carers written permission. Advice on this is available on the Durham Extranet- Template Photographic policy

- Villa Real School will ensure that all images and videos shared online are used in accordance with the School's photographic/ image policy and the data protection act.
- Villa Real School will ensure that all use of images and videos take place in accordance other policies and procedures, including data security, Acceptable Use policies, Codes of conduct; social media, use of personal devices, school systems etc.

- In line with the image policy written permission from parents/ carers will **always** be obtained before images/ videos of pupils/ students are electronically published
- Media held on school devices will be periodically be cleansed in order to safeguard images and videos of current and past pupils

Managing Email; School Community (To be read alongside Appendix A
Professionals must ensure that their use of email at work always complies with data protection legislation and confidential or personal data must not be sent electronically unless appropriately encrypted/ pass worded. Staff must be appropriately trained and SMT must ensure all staff; where appropriate are provided with and are using appropriate, secure email systems and passwords to share any personal/ sensitive data and or information. Pupils/ students; where appropriate may have access to their own school email address for educational purposes. These email accounts are or will be carefully considered in appropriateness as revealing pupil/ student names may expose them to identification by unsuitable persons or people. It is likely that whole class or project email addresses will be used for educational purposes

- Pupils/ students may only access and use Villa Real School email accounts for educational purposes in school time/ learning time (not for EYFS)
- Whole class/ project group email addresses may be used for communication outside of the School - monitored by class staff/ project lead
- Email accounts will be deleted upon a pupil leaving Villa Real School. Any work held on these accounts will be permanently lost.

Staff Email management (To be read alongside Appendix A)

- All members of staff are provided with a specific email address, username and set an individual secure password themselves
- The use of personal email addresses by staff for any official school business is not permitted
- 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 which contains any content which could be subject to data protection legislation (sensitive/ personal information) will only be sent using secure school email address and where technically possible or required encrypted
- Access to school email systems will always take place in accordance with data protection legislation and in line with other appropriate school policies
- Members of the School Community must inform a designated member of staff if they receive offensive communication and this will be recorded in the School's Safeguarding files/ records

- Staff will be encouraged by SMT to develop an appropriate work/ life balance when responding to email relating to work. This is especially important where communications are taking place outside of school hours and is taking place between staff and parents/carers. Staff will not be expected to answer emails outside of normal working hours but may send or schedule send emails at any time.
- Excessive social email use can interfere with teaching and learning and, may be restricted.
- Staff are not expected to stop teaching to answer emails. However, if a teacher feels they have a quiet moment they may. School emails between staff should not be visible on interactive white boards.
- Staff access personal email accounts using school devices is not permitted unless permission sought from Headteacher or Deputy Head teacher prior to accessing personal email account
- Emails sent to external organisations should be written professionally and carefully and where required authorised before sending
- The School email addresses and other official contact details will not be used for setting up personal accounts or personal social media accounts

Official video conferencing and webcam use for educational purposes (To be read alongside Appendix A)

Video conferencing enables users to see and hear each other in different locations. This 'real time' interactive technology has many uses in education. This can be a useful tool to allow pupils/ students to explore and source new experiences

- The School acknowledges that video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity
- All video conferencing equipment will be switched off when not in use and where appropriate, not set to auto answer
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name
- External IP addresses will not be made available to other sites
- Video conferencing contact details will not be posted publicly
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use
- School video conferencing equipment will not be taken off the School's premises without authorisation from SMT
- Staff will ensure that external video conference opportunities and or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure

Video Conferencing Users

- Pupils/ students will ask permission from a teacher before making or answering a video conferencing call or message
- Video conferencing will be supervised appropriately for the pupils age and ability- (this will be tasked to individual class teachers and staff using the guidelines set out in this policy)
- Parents/ carers written consent will be obtained prior to pupils/ students taking part in video conferencing activities
- Video conferencing will take place via official and approved communication channels following a robust risk assessment
- Only key administrators will be given key access to video conferencing administration areas or remote control pages
- Unique log on and password details for the educational video conferencing services will only be issued to members of staff and kept secure

Video Conferencing Content

- When recording a video conference lesson, written permission will be given by all sites and participants
- The reason for the recording must be given and the recording of the video conference should be clear to all parties at the start of the conference
- Recorded materials must be stored securely
- If third party materials are to be included, the School will check that recording is acceptable to avoid infringing the third party intellectual property rights
- The School will establish dialogue with other conference participants before taking part in a video conference. If it is a non-school site the School will check that they are delivering material that is suitable for the class

Appropriate and safe classroom use of the internet and any associated devices. (To be read alongside Appendix A)

All members of staff must be aware that no search engine or filtering tool is ever completely safe, and appropriate supervision, use of safe search tools (where possible), pre checks of search terms, age appropriate education for pupils and robust classroom management must always be in place. However, despite these steps pupils/students may still be exposed to inappropriate materials therefor SMT must ensure there are clear procedures for reporting access to unsuitable content, which staff, pupils/ students must be aware of.

Villa Real School permits pupils/ students to bring in and use their own electronic devices on site in a non-educational capacity. This is explicitly risk assessed and supported with clear policy, guidelines and procedures including pupil/ student AUP policy

- Internet use is a key feature of educational access and all pupils/ students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum (subject specific overview will provide further information)
- Villa Real School's internet access will be designed to enhance and extend education
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils/ students
- All members of staff are aware that we cannot rely on filtering alone to safeguard pupils/ students and supervision, classroom management and responsible use is essential
- Supervision and management of pupils/ students will be appropriate to their age and ability
- At Early Years Foundation Stage and Key Stage 1: pupils' access to the internet will be adult led or through adult demonstration with direct supervised access to specific and approved online materials which supports the learning outcomes planned for pupils age and ability
- At Key Stage 2: will be closely supervised accordingly and will only access age appropriate search engines and online tools and online activities which will be teacher led or teacher directed where necessary.
- Pupils/ students will be directed to online materials and resources which support the learning outcomes planned for the pupils'/ students' age and ability
- Senior and sixth form students will be appropriately supervised when using technology according to their ability and understanding
- All school owned devices will be used in accordance with the School Acceptable Use Policy with appropriate measures in place
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for home learning-homework
- Pupils/ students; where appropriate will be educated in the effective use of the internet in research including the skills of knowledge, location, retrieval and evaluation
- The School will ensure that the use of internet derived materials by staff and pupils/students complies with copyright law and acknowledge the source of the information
- The School will ensure that the safety features are enabled on adult sites which the staff direct the pupils/ students to use (google safe search, YouTube safety mode)

- Pupils/ students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of online materials is part of teaching and learning in every subject and will be viewed as a whole school setting requirement across the curriculum
- The School will use the internet to enable pupils/ students and staff to communicate and collaborate in a safe and secure environment

Management of school learning platforms/portals/gateways

An effective learning platform or environment can offer schools/settings a wide range of benefits, as well as support management and administration. It can enable staff to communicate effectively across schools or settings pupils/ students to share work across schools, the sharing of resources, capture progress and create work. The above must be used subject to careful monitoring by SMT. Senior Managers have a duty to review and update the policy regarding the use of the learning platform, and all users must be informed of any changes made.

- SMT and appropriate staff will regularly monitor the usage of the learning platform in particular message and communication tools and publishing facilities
- Staff, pupils/students will be advised about acceptable use and appropriate conduct when using the learning platform
- Only members of the current school community, including parents/ carers will have access to the learning platform
- All users will be mindful of copyright issues and will only upload appropriate content to the learning platform
- When staff, pupils/students leave the School their accounts or rights to specific school areas will be disabled and if appropriate transferred to their new establishment

Any concerns about the content on the learning platform will be recorded and dealt with in the following ways:

- The user will be asked to remove any materials deemed in appropriate or offensive
- The material will be removed by the site administrator with a member of the SMT
- Access to the learning platform may or will be suspended
- The user will ned to discuss the issues with a member of SMT before reinstatement
- A pupils'/ students' parents or carer may need to be informed
- A visitor may be invited onto the learning platform by a member of leadership. In this instance there will be a focused time and limited time slot

- Pupils/students may require editorial approval from a member of staff. This may be given to a pupil to fulfil a specific aim and will have a limited time frame for completion

General Social Media use & Staff use of Personal Social Media Accounts

Villa Real School acknowledges that there are significant potential benefits for communication, engagement, collaboration and learning via the internet and social media. However, the School also recognises the risks associated with users (staff, pupils/ students and the wider school community)

- Expectations regarding safe and responsible use of social media will apply to all member of Villa Real School Community and exist in order to safeguard both the School and the wider school community, on and off line
- Staff must not be friends on social media sites with parents/ carers
- Staff are aware it is not acceptable to send or receive messages over social media/ messenger sites about matters relating to any aspects of pupils'/ students' school life or school life in general
- Staff must report to SMT if or when a parent/ carer has contacted them personally via social media/ messenger platform about a pupil/ student in their care
- It is not acceptable that staff use any school device to access their social media profile/ feed or messenger platform
- All members of Villa Real School Community will be encouraged to engage in social media in a positive, safe and responsible manner at all times
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Villa Real School Community
- All members of the Villa Real School Community are advised not to publish specific and detailed private thoughts, concerns, opinions, pictures or messages on any social media services especially content that may be considered threatening, hurtful, offensive, or defamatory to others and the School
- Villa Real School will control pupil/student and staff access to social media and social networking sites whilst online
- The use of social networking applications during school time is permitted during staff break times
- Inappropriate or excessive use of social media during school work hours and not at permitted times may result in disciplinary action
- Any concerns regarding the online conduct of any member of Villa Real School Community on social media sites should be reported to the SMT (Senior Management Team) and will be managed in accordance with the relevant policies and procedures
- Any breaches of Villa Real School policy may result in criminal, disciplinary or civil action been taken and this will depend upon the age and role of those involved and the circumstances of the wrong

committed. Action will be taken in accordance with the relevant policies and procedures e.g. safeguarding and code of conduct policies

- 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 and 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 Villa Real School's Acceptable Use Policy
- All members of staff are advised not to communicate with or add 'friends' and current/ past students or pupils or family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions which may compromise this will be discussed with the Designated Safeguarding Lead or the Headteacher
- If ongoing contact with pupils/students is required once they have left the School roll, then members of staff are expected to use existing alumni network or school approved communication tools
- All communication between staff and members of the School Community will take place via official approved communication channels
- Staff will not use personal social media accounts to make contact with pupils, students, parents, carers or the afore mentioned extended family members except where specific permission has been sought from the Headteacher
- Any communication from pupils/ students, parents/ carers received on social media accounts will be immediately reported to the Headteacher
- Information and content that staff have access to as part of their employment, including photos and personal/sensitive information about pupils/ students and their families will not be shared or discussed on social media sites
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, privacy settings and opting for the strictest levels of security, ensuring their professional role is protected and is in accordance with the School's policies, Safeguarding Policy. (Confidentiality Policy, Data Protection Policy) and the wider professional and legal framework
- Members of staff will be encouraged to manage and control the content they share and post online
- Advice will be provided to staff via regular training and by sharing appropriate guidance and resources on a regular basis
- Members of staff will notify the SMT immediately if they consider that any content shared or posted via any information and communications technology, including email or social networking sites conflicts with their role at Villa Real School

- Members of staff are encouraged not to identify themselves as employees of Villa Real School on their personal networking accounts. This is to prevent information on these sites being linked with Villa Real School and also to safeguard the privacy of staff members and the wider school community
- Staff members will ensure that they do not represent their personal views as that of Villa Real School on social media
- Villa Real School email addresses will not be used for setting up personal social media accounts
- Members of staff who follow the official school Facebook page will be encouraged and advise to set their social media account settings on the highest security level possible or use official professional accounts- to avoid blurring professional boundaries

Artificial Intelligence

Acceptable Use of AI by as advised by the DFE

1. Permitted Uses

Teachers are encouraged to use AI tools for:

- Lesson planning and curriculum design
- Creating teaching resources (e.g. worksheets, quizzes, presentations)
- Marking and feedback (especially low-stakes tasks)
- Generating differentiated materials for SEND learners
- Administrative tasks (e.g. reports, emails, timetables)
- Professional development (e.g. summarising research, drafting CPD materials)

---

2. Professional Judgement

- Teachers must review and verify all AI-generated content for accuracy, appropriateness, and bias.
- AI should support, not replace, teacher expertise or relationships with students.
- Final responsibility for content and decisions always rests with the teacher and school.

---

3. Safeguarding and Data Protection

- Do not input personal, identifiable, or sensitive data (e.g. student names, photos, medical info) into AI tools.
- Avoid uploading student work unless parental consent is obtained and the tool complies with UK GDPR.
- Ensure AI tools used are age-appropriate, secure, and filtered to prevent exposure to harmful content.

---

4. Transparency and Ethics

- Be open about using AI in teaching—model responsible use for students.
- Avoid using AI to detect plagiarism or AI-generated student work unless tools are proven reliable.
- Do not use AI to generate student reports or grades without human oversight.

---

5. School Policy Alignment

- Use of AI in line with your school's Acceptable Use Policy, Safeguarding Policy, and AI Policy
- Work must comply with legal duties around:
    - Child safety
    - Data protection
    - Intellectual property

---

6. Training and Support

- Teachers will receive regular training on:
    - AI capabilities and limitations
    - Ethical and safe use
    - Risks such as bias, misinformation, and over-reliance

❌ Unacceptable Uses

- Uploading personal or sensitive data without consent
- Using AI to replace teacher judgement in grading or safeguarding
- Relying on AI for high-stakes decisions (e.g. exclusions, referrals)
- Using AI tools that lack transparency, safety filters, or age-appropriate design

Official Social Media use

Villa Real School's Official Facebook page

- Official use of social media sites by Villa Real School will only take place with clear educational or community engagement objectives with specific outcomes, e.g. increasing parental engagement, information of school events
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher
- Villa Real School's social media channel- Facebook will be set up as a distinct and dedicated social media site for educational, information and engagement purposes
- Staff will use Villa Real School's provided email address to register for and manage any official approved social media channels - Facebook
- Members of staff running the School's official media site- Facebook will sign a specific acceptable use policy to ensure they are aware of the required behaviours and expectations of use and ensure that the sites are used safely, responsibly and in accordance with local and national guidance and legislation
- All communication on school official Facebook page will be clear, transparent and open to scrutiny
- Any online publication on official social media sites will comply with legal requirements including the Data protection act 1998, right to privacy conferred by the Human Rights Act 1998 or similar duty to protect private information and will not breach any common law duty of confidentiality
- Official social media use- Facebook will be in line with existing policies including anti bullying and child protection
- Images or videos of pupils/students will only be shared on school official Facebook site in accordance with the current adopted photographic/ images policy
- Information about safe and responsible use of Facebook page and other social media channels will be communicated clearly and regularly to all members of the School Community
- Official social media sites, blogs or wikis will be suitably protected and where possible / appropriate, run and or linked from the School's official website and take place with written approval from the SMT

- Leadership staff must be aware of account information and relevant details for the School Facebook page in case of an emergency - staff absence
- Parents/ carers and pupils/ students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the School community
- Public communications on behalf of Villa Real School on official Facebook page, where possible, all content uploaded will be agreed by at least one other colleague
- School's official Facebook page will link back to the School's website and the School's Acceptable Use Policy to demonstrate the account is official
- The School will ensure that any official social medial use does not exclude members of the School community who are unable or unwilling to use social media platforms
- If members of staff are participating in online activity as part of their capacity as an employee of Villa Real School, they are requested to be professional at all times and to be aware that they are an ambassador for the School
- Staff using social media officially will disclose their official role/ position but always make it clear that they do not necessarily speak on behalf of the School
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright as well as equalities laws
- Staff must ensure that any images or videos posted on any official social media channel have appropriate written parental consent
- Staff using social media officially will be accountable and not disclose information, make comments or engage in activities on behalf of the School unless authorised to do so from the Headteacher
- Staff using social media officially will inform the Headteacher of any concerns such as criticism or inappropriate content posted online
- Staff using social media officially will not engage with any direct or private message with pupils/ students, parents/ carers through social media and will communicate via official communicative channels
- Staff using social media officially within the School will read and sign the School social media Acceptable Use Policy

Pupils'/students' use of Social Media

Social media is now an everyday form of communication for many children and young people and forms a vital part of growing up in today's modern Britain and the wider global society. Whilst many educational settings choose

to block access to social media sites in school, it cannot be assumed that they will not access them offsite using personal devices.

- Safe and responsible use of social media sites will be outlined for pupils/ students, parents/carers as part of the Acceptable Use Policy
- Personal publishing on social media sites will be taught to pupils/ students as part of an embedded and progressive education approach via age-appropriate sites which have been risk assessed and approved suitable for educational purposes
- Pupils/ students will be advised to consider the risks of sharing personal detail of any kind on social media sites which may identify them and their location e.g., name, school names of family members
- Pupils/ students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present
- Pupils/ students will be advised on appropriate security on social media sites and will be encouraged to use safe and secure passwords, deny access to unknown individuals and will be supported in learning how to block and report unwanted communications
- Pupils/ students will be encouraged to approve and invite known friends and family only on social networking sites and deny access to others by making their profiles private/ protected
- Parents/ carers will be informed of any official social media use with pupils and written parental consent will be obtained prior to access as required
- Any official social media activity involving pupils will be moderated by the School where possible
- The School is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for pupils/students under this age
- Any concerns regarding pupils/ students' use of social media and personal publishing sites, both at home and school, will be dealt with existing school policies including anti bullying
- Any concerns regarding pupils' use of social networking social media and personal publishing sites, both at home and at school, will be raised with parents/ carers particularly when concerning any underage use of social media sites

Use of Personal Devices and Mobile Phones

Mobile phones and other personal devices such as tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops are considered to be an everyday item in today's society.

Rational and expectations for safe use of personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among pupils/ students and adults will require all members of Villa Real School Community to take steps to ensure that mobile phones and personal devices are used responsibly
- The use of mobile phones and other personal devices by pupils/ students will be decided by Villa Real School and is covered in the appropriate policies – including Acceptable Use Policy
- Villa Real School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils/ students, parents/ carers and staff but requires that such technologies need to be used safely and appropriately within school
- All use of personal devices and mobile phones will take place in accordance with the law and the following school policies
  Data Protection policy 2018
  Keeping Children Safe in School policy
  Pupil Acceptable Use policy
  Staff Acceptable Use policy
  Photographic and Images policy
- Electronic devices of all kinds that are brought on site are the responsibility of the user at all times. Villa Real School accepts no responsibility for the loss of or damage to such items. Nor will Villa Real School accept responsibility for any adverse health effects caused by any such devices either potential or actual
- Mobile phones and personal devices are not permitted to be used in certain areas within the School or off site such as; classrooms, toilets, corridors, changing rooms, swimming pools
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the current Disciplinary Policy
- Members of staff will be issued with work contact details, contact number, email address and where necessary a work phone in case contact with parents/ carers is required
- All members of the Villa Real School Community will be advised to take steps to protect their mobile phones and personal devices from loss or damage
- All members of the Villa Real School Community will be advised to use pin numbers/ passwords to ensure any unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.
- Passwords and pin numbers are to be kept confidential and not shared
- All members of Villa Real School Community will be advised that their mobile phone/ personal devices do not display/ contain any content which may be considered to be offensive, derogatory or would otherwise contravene relevant Villa Real School policies

- Mobile phones and personal devices must always be used in accordance with Villa Real School's Acceptable Use Policy
- Villa Real School mobile phones and devices are only to be used by school employees and must be protected via password/pin and must only be accessed to contact parents/ carers or school business

Pupils'/students' acceptable use of personal devices and mobile phones

- Pupils/ students will be educated regarding the safe and appropriate use of mobile phones and personal devices
- All use of personal devices and mobile phones by pupils/students will take place in accordance with the Acceptable Use Policy
- Pupils/ students personal devices and mobile phones will be kept in a secure place, switched off and kept out of sight during lessons and only be used at agreed times and in SMT agreed locations within the School
- If members of staff have an educational reason to allow pupils/ students to use a personal device or mobile phone as part of an educational activity, then specific permission will be sought from SMT. This will be decided on an individual basis
- Pupils/ students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of possible consequences and boundaries
- If a pupil/ student breaches school policy, then the device will be confiscated and will be held in a secure place in the School office. Mobile phones and devices may be released to parents/ carers in accordance with school policies
- School staff may confiscate a pupil/ student's mobile phone or device if it is being used to contravene the School's anti bullying policy, behaviour policy or could contain Youth Produced Sexual Imagery. The phone or device may be searched by a member of the safeguarding team or SMT with the consent of the pupil/ student or parent/ carer and if appropriate will be deleted. This will be carried out in accordance with procedure https://www.gov.uk/government/publications/searching-screening-and-confiscation

Staff Safe and Acceptable Use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting pupils/ students and their families within or outside the setting in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with the Headteacher
- Staff will not use personal devices, cameras, tablets or mobile phones to take videos, photos or images of pupils/students
- Only equipment provided by the School, and pass worded, may be used to take videos, photos, images of pupils/ students for this purpose
- Members of staff will ensure that any use of mobile phones and personal devices will always take place in accordance with the law; data

protection, confidentiality, acceptable use, keeping children safe in school photographic/ images policies

- Staff will not use any personal devices or mobile phones directly with children and will only use school provided equipment
- Staff personal devices and mobile phones will be either switched off/ or switched to silent mode during lesson times
- Staff will store personal devices and mobile phones away securely during contact time with pupils/ students
- Blue tooth and other forms of communication should be hidden or switched off during lesson times
- Staff may take personal mobile phones on outdoor visits/ offsite activities but are only to be used in an emergency -or if all other communications fail
- If a member of staff is thought to have illegal content saved or stored on their mobile phone or personal device or have committed a criminal offence then the police will be contacted
- Any allegations against members of staff involving personal use of mobile phone or other personal devices will be responded to following the School's Allegations Management Policy

Visitors' use of personal devices and mobile phones

- Parents/ carers and visitors must use mobile phones and personal devices in accordance with the School Acceptable Use Policy
- Use of mobile phones or personal devices by visitors and parents/ carers to take photos, images or videos must take place within the procedures and guidelines set out in the School's Photographic/ Images Policy
- The School will ensure appropriate information is disseminated to inform all visitors in school of the expectations of use
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breach by visitors

Reducing online risks

Many emerging communications technologies offer the potential to develop new teaching and learning tools including mobile communications, internet access and multimedia tools. A risk assessment will be undertaken regarding each new technology for effective safe classroom practice to be developed.

Use of Mobile Phones and Personal Devices

- Parents, carers, and visitors must use mobile phones and personal devices in accordance with the **School's Acceptable Use Policy**.
- Taking photos, images, or videos by visitors and parents/carers must follow the procedures and guidelines set out in the **School's Photography and Images Policy**.
- The School will ensure that all visitors are informed of these expectations through appropriate signage, briefings, and visitor information.
- Staff are expected to challenge inappropriate use when it is safe and appropriate to do so and must report any breaches by visitors to the **Designated Safeguarding Lead (DSL)** immediately.

Reducing Online Risks

Emerging communication technologies offer opportunities for innovative teaching and learning, including mobile devices, internet access, and multimedia tools. To ensure safe practice:

- A **risk assessment** will be carried out for each new technology before it is introduced for classroom use.
- Villa Real School recognises that the internet is a constantly changing environment with new apps, tools, devices, and platforms emerging rapidly.
- All emerging technologies will be evaluated for educational benefit, and the Senior Management Team (SMT) will ensure appropriate risk assessments are completed before use is permitted.
- The School will maintain **appropriate filtering and monitoring systems** to prevent staff and pupils from accessing unsuitable or illegal content.
- The School will take all reasonable precautions to ensure users access only appropriate material. However, due to the global nature of the internet, it is not possible to guarantee that unsuitable material will never be accessed via a school device.
- The School will **audit technology use** regularly to ensure the Online Safety Policy remains effective and properly implemented.
- Methods to identify, assess, and minimise online risks will be reviewed regularly by the **Senior Management Team**

Internet use throughout the wider school and community

Internet access is available in many situations in our local community, in addition to school and home.

- The School will liaise with local organisations to establish a common approach to online safety
- The School will work with the local community's needs (whilst recognising cultural backgrounds, languages, religions and ethnicity)

- The School will provide an Acceptable Use Policy for any guest/visitor who needs to access the School computer system or internet on site

Authorising Internet Access

Villa Real School allocates internet access to staff and pupils/students on the basis of staff requirements, roles, responsibilities and for pupils'/students' educational needs. However, there may be some pupils/ students who are denied access. Access is given on an individual basis to staff and pupils/ students. Visitors/ guests to the setting use the 'Guest' password and username if they require access to the internet whilst in school.

- All staff, pupils/ students and visitors will read and sign the Acceptable Use Policy before using any school resources
- Parents/ Carers will be informed that pupils/ students will be provided with supervised internet access which is appropriate to their age and ability
- Parents/ carers will be asked to read the Pupil/ Student Acceptable Use Policy for pupil access and discuss it with their child, where appropriate
- When considering access for the pupils/ students the School will make decisions based on the specific needs and understanding of the pupils/students

Engagement and education of pupils/ students

Online safety is an important part of the computing curriculum programmes of study for pupils/ students within schools and this only highlights the importance for pupils/students to use technology safely and respectfully, understand how to keep personal information private and be able to identify where to go for help and support when they have concerns on the internet or other online technologies from an early age, and where appropriate based on pupil/student age, ability and development. Pupils/students need to learn digital literacy and refine their own publications/ communications with others via the internet. Pupils/ students will need to be taught how to develop an understanding on how to become and stay safe, responsible and respectful online and become positive digital citizens. The Computing Curriculum will form part of online safety education for pupils/ students safe and responsible use of technology embedded throughout the whole school curriculum to ensure pupils/ students develop the required range of digital literacy skills, safety skills and develop online resilience enabling them to become confident, safe, responsible internet users

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils/students

- Education about safe and responsible use will precede internet access
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability
- All users will be informed that network and internet use will be monitored
- Online safety will be included in RSE, PSHCE, Citizenship and Computing programmes of study, covering both safe school and home use
- Pupils/ students may be sought when writing and developing school online safety policies and practices, including curriculum development and implementation
- Acceptable use expectations will be posted in each classroom along with SMART safety rules
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas
- External support will be used to complement and support the School's internal online safety approaches
- The School will reward positive use of technology by pupils/students
- The School will implement peer education to develop online safety as appropriate to the needs of the pupils/students

Suggested / Useful Online Safety Programmes

- **ThinkUKnow** – https://www.thinkuknow.co.uk
  (CEOP's education programme for children, parents, and professionals)
- **Childnet** – https://www.childnet.com
  (Resources for schools, parents, and young people on safe internet use)
- **Internet Matters** – https://www.internetmatters.org
  (Guidance for parents and schools on online safety and digital wellbeing)
- **UK Safer Internet Centre** – https://www.saferinternet.org.uk
  (Classroom resources, policy templates, and advice for educators)
- **SWGfL Digital Literacy Toolkit** – https://swgfl.org.uk/resources/digital-literacy

Engagement and education of pupils/students considered to be vulnerable

Pupils/students may be considered to be vulnerable for a variety of reasons. This includes pupils/ students with special educational needs, mental health needs, looked after, who have experienced trauma and abuse, hardship, low self-esteem or with an additional language

- Villa Real School is aware that some children may be considered to be more vulnerable online due to a range of factors

- Villa Real School will ensure that differentiated and ability appropriate online safety is given with input where necessary from specialist staff (e.g. SENCO, Safeguarding lead)
- All victims are provided with appropriate support and reassured that the case is taken seriously. They should never feel ashamed

Engagement of parents and carers

Parents and Carers form a vital element in the approach to teaching and empowering pupils/ students to become safe and responsible digital citizens. By working together parents, carers and Villa Real School along where appropriate with other professionals can help reinforce online safety messages and encourage positive behaviour online

- Villa Real School recognise that parents/carers have an essential role to play in enabling pupils/students to become safe and responsible users of the internet and digital technology
- Parents/ carers attention will be drawn to the School Online Safety Policy and expectations in newsletters or on the School website
- A partnership approach to online safety at home and at school with parents/ carers will be encouraged. This may include offering parents evenings with demonstrations, suggestions and support for safe home internet usage
- Parents/ carers will be encouraged to read the School Acceptable Use policy for pupils/ students and discuss its implications with their child/ children
- Information and guidance for parents/ carers on online safety will be made available on the School website

Technical Security

The responsibility for managing the technical environment is ultimately the responsibility of the Headteacher and Governing Body. The responsibility for the use of a shared engineer/service provider to support, maintain and develop infrastructure is the responsibility of the Headteacher and Governing Body

- The security of the School information systems and users will be reviewed regularly
- Virus protection will be uploaded regularly
- Portable media may not be used without specific permission followed by an anti-virus/ malware scan
- Unapproved software will not be allowed in work areas or attached to email
- Files held on the School's network can be checked
- The network manager will review system capacity regularly
- The appropriate use of user logins and passwords to access the School network will be enforced for all but the youngest users

- All users are expected to log off or lock screens/ devices if systems are unattended

Passwords

- All staff/ users are aware not to share passwords or information with others and not to log in as another user at anytime
- Staff must always keep passwords/ logins private and must not share with others or leave it where others can find it
- All members of staff will have their own unique usernames and passwords to access school systems and where appropriate LA systems
- All members of staff are responsible for keeping their passwords, usernames, logins private
- Passwords must be at least 8 characters long
- Passwords contain at last 1 upper case and 1 lower case letter
- Passwords 1 number or punctuation character
- NOT be a dictionary word
- All staff are aware that passwords, usernames, logins are not to be shared with pupils/students or visitors
- Any visitors must use the generic visitor password if access is required to school digital systems or internet
- Passwords, usernames, logins are compulsory throughout Villa Real School
- Passwords, usernames, logins must be changed on notification; failure to do so may result in accounts being temporarily disabled. Please notify systems manager
- Staff are aware if they cannot remember their password, username or login to notify systems manager and instructions will be given as to how to reset securely other colleagues or outside agencies e.g. NHS, SALT
- Passwords must not be shared

Filtering and Monitoring

Keeping children safe in education 2025 states, '*Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of designated safeguarding lead…. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).*'

- The governing body will ensure that the School has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit pupils'/students' exposure to online risks
- The School's internet access strategy will be dependent on the need and requirements of our community and will there for be designed to suit the age and curriculum requirements of our pupils/students, with advice where appropriate from technical, educational and safeguarding staff

- All monitoring of school owned/ provided systems will take place to safeguard members of the School community
- All users will be informed that the use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation
- The School uses educational filtered secure broadband connectivity through Durham County Council
- The School has clear procedure for reporting breaches of filtering which all staff, pupils/ students, are aware of
- If staff pupils/ students discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead Jill Bowe and will then be recorded and escalated as appropriate
- The School filtering system will block all sites on the **Internet Watch Foundation** list
- Changes to the School's filtering policy will be risk assessed by staff with educational and technical experience prior to any changes where appropriate with consent from the SMT
- All changes to the School filtering systems/policy will be recorded
- The SMT will ensure regular checks are made to ensure that the filtering methods selected are effective and appropriate
- Any materials that the School believes is illegal will be reported to appropriate agencies such as the Police or CEOP immediately

Management of applications used to record pupils'/ students' progress

- Any use of cloud based systems will follow guidance from the ISO
- The Headteacher is ultimately responsible for the security of any data of images held of pupils/ students
- Apps/ systems which store personal/sensitive data will be risk assessed by SMT prior to use
- Only Villa Real School issued devices will be used for apps which record and store pupils/students personal or sensitive data
- Personal devices or mobile phones will not be used to access or upload content to any apps which record or store pupils'/ students' attainment, personal/ sensitive information or data
- Devices will be appropriately encrypted or password protected if taken off site to prevent a security breach in the event of loss or theft
- Users will be advised on safety measures to protect all members of the School community such as using a strong password, logging out of systems and so on
- Parents/ carers will be informed of the School's expectations regarding safe and appropriate use prior to being given access (not sharing passwords/ images)

Responding to online incidents and safeguarding concerns

Online safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Potential concerns an often be dealt with at a personal level by ensuring a pupils/students are able to identify and speak with a trusted adult.

Staff must also be vigilant about their own behaviour and other colleagues' behaviour on and offline, reporting any concerns noticed should be encouraged to develop a safe culture.

- All members of the School community will be made aware of the range of online risks that are likely to be encountered including sexting, online cyber bullying etc. This will be highlighted in staff training and educational approached for pupils/ students
- All members of Villa Real School will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will be recorded
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with DSCP systems
- If there is a possibility that an offence has occurred, then any equipment used should be isolated and left unused to preserve any evidence on the device
- Complaints about the internet will be dealt with under the School's complaints procedure
- Complaints about online cyber bullying will be dealt with under the School's anti bullying policy and procedure
- Any complaint about staff will be referred to the Headteacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (local authority designated officer)
- Pupils/ students, parents/ carers and staff will be informed of the School's complaints procedure
- Staff will be informed of the complaints and whistleblowing procedure
- All members of the School community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns
- All members of the School community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to the School or any other members of the School community
- The School will manage online safety incidents in accordance with the School policy and procedures where appropriate
- The School will inform parents/ carers of any incidents as and when required
- After investigations are completed the School will debrief, identify lessons learnt and implement any changes as required

- Where there is cause for concern or fear that illegal activity has or is taking place then the School will contact Durham Police via local Police station or EDP
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Durham Police
- If the School is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team
- Parents/ carers and their child/ children will need to work in partnership with the School to resolve issues

Responding to concerns regarding online child sexual abuse and exploitation

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or sexually exploited via the internet. Typically referred to as 'online grooming', however this term can be often considered as too narrow as it implies 'grooming behaviour ' has taken place over some time whilst offender has gained trust and built a relationship with the victim.

2.2.11 Safeguarding children abused throughout sexual exploitation

- Villa Real School will ensure that all members of the School community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children/ young people and how to respond to concerns
- Villa Real School will implement preventative approaches for online sexual abuse via a range of age and ability appropriate educational approaches for pupils, students, staff, parents and carers
- Villa Real School views online sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with the DSL Jill Bowe Headteacher
- If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately. If the School are made aware of an incident regarding a child sexual abuse of a child/ young person in the School; then the School will:
- Act in accordance with the School's child protection policy and relevant DSCP procedures
- Immediately notify the designated Safeguarding Lead- Jill Bowe
- Store any devices involved securely
- Immediately inform Durham Police via 111 (999 if child is an immediate risk)
- Where appropriate the School will involve and empower pupils/ students to report concerns regarding online sexual abuse e.g. using CEOP report form www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerability of pupils/ students involved; this includes carrying out checks with other agencies

- Make referral to First Contact (if needed/ appropriate)
- Put the necessary safeguards in place for pupils/ students e.g. offer counselling support and immediate protection, offer appropriate pastoral support for those involved
- Inform parents/ carers about the incident and provide details of how situation is being managed
- Review the handling of any incidents to ensure the School is implementing best practice and the School leadership team (SMT) will review and update any management procedures where necessary

Responding to concerns regarding indecent images of children

Villa Real School must be aware of and understand the law regarding indecent images of children specifically but not limited to:

- The sexual offences Act 2003 (England & Wales) defines a child for the purposes of indecent images as anyone under the age of 18
- Villa Real School will ensure that all members of the School community are made aware of the criminal nature of indecent images of children including possible consequences
- The School will take action regarding of indecent images of children regardless of the use of Villa Real School equipment or personal equipment both on and off site
- The School will take action to prevent access and or accidental access to of indecent images of children e.g. using an internet provider who is subscribed to the INTERNET WATCH FOUNDATION BLOCK, implementing appropriate and effective web filtering, implementing firewalls and anti-spam software
- If the School is unclear if a criminal offence has been committed the DSL Jill Bowe will obtain advice immediately through the Educational Safeguarding team

If the School is made aware of indecent images of children the School will:

- Act in accordance with the School's child protection and safeguarding policy
- Immediately notify the School DSL - Jill Bowe
- Store any devices involved securely
- Immediately inform appropriate organisations (e.g. Internet Watch Foundation, Durham Police 101 or 999 if child is at immediate risk, LADO if there is an allegation against a member of staff)

If the School are made aware that a member of staff, pupil, student had been inadvertently exposed to indecent images of children whilst using the internet 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 that any copies that exist of the image, e.g. emails are deleted

- Sexual harassment of peers through sharing indecent images and other harmful content is monitored and interventions planned as part of safeguarding

If the School is made aware that indecent images of children have been found on the School's electronic devices, then the School will:

- Ensure the DSL is informed Jill Bowe
- Ensure the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, e.g. emails are deleted
- Inform Durham Police via 111 or if there is an immediate risk of harm to the child 999 and social services if appropriate
- Only store copies of the images at the request of the police only (images to be stored securely, all other copies must be deleted)

If the School are made aware that a member of staff is found in possession of indecent images of children on their electronic device, provided by the School then the School will:

- Ensure the DSL Jill Bowe is informed or another member of staff in accordance with the School whistle blowing procedure
- Contact the Police regarding the images and quarantine any devices until Police advice has been sought
- Inform the local authority LADO and other relevant organisations in accordance with the School's managing allegations policy
- Follow appropriate school policies regarding conduct

Responding to concerns regarding radicalisation and extremism online

From 1st July 2015 specified authorities including all schools are subject to a duty under 26 of the Counter- Terrorism and Security Act 2015 in the exercise of their functions, to have due regard to the need to prevent people from being drawn into Terrorism. This duty is known as 'The Prevent Duty'.

The Prevent Team can be contacted: graham.mcardle@durham.gov.uk
Useful links regarding radicalisation and extremism
DfE: www.educateagainsthate.com
Report online hate and terrorism: http://course.ncalt.com/channel General Awareness
National Helpline: 020 7340 7264

- The School will take all reasonable precautions to ensure that pupils/ students are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of the pupils- see internet usage by pupils/ students/ monitoring of
- When concerns are notes by staff that a pupil/student may be at risk of radicalisation online then the Designated Safeguarding Lead - Jill Bowe

will be informed immediately and action will be taken in line with the safeguarding policy
- Online hate content directed towards or posted by specific members of the School community will be responded to in line with existing school policies including anti bullying, safeguarding. If the School is unclear if a n offence has been committed the DSL- Jill Bowe will obtain advice immediately via the Education Safeguarding Team

Responding to concerns regarding cyberbullying

Online bullying can be defined as the use of information technology, particularly mobile phones to deliberately hurt or upset someone
Additional information can be found at:
https://www.gov.uk/goverment/publications/preventing-and-tackling-bullying

- Cyberbullying along with all other forms of bullying, of any member of Villa Real School Community will not be tolerated. Full details are set out in school policy Anti bullying
- All incidents of online bullying will be recorded
- There are clear procedures in place to investigate incidents or allegations and support anyone in the School community affected by online bullying
- If the School is unclear if a criminal offence has been committed, then the DSL Jill Bowe will obtain advice immediately from Durham Police
- Pupils, students, parents, carers and staff will be advised to keep a record of cyberbullying as evidence
- The School will take steps to identify the bully/ bullies where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary
- Pupils, students, parents, carers and staff will be required to work with the School to support the approach to cyberbullying and the School's online safety ethos

Sanctions for those involved in cyberbullying:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove the content if those involved refuse or unable to delete content
- Internet access may be suspended at school for the user for a period of time, other sanctions for pupils, students and staff may also be used in accordance with the School's Anti Bullying Policy, Acceptable Use Policy, Code of Conduct
- Parents/carers of the pupil/ student involved in the online bullying incident will be informed
- The Police will be contacted if a criminal offence is suspected

Responding to concerns regarding online hate

Hate crimes are any crimes that are targeted at a person because of hostility or prejudice towards that person:

- Disability
- Race or ethnicity
- Religion or belief
- Sexual orientation
- Transgender identity
- Online hate at Villa Real School will NOT be tolerated. Further details regarding the above are set out in the School's Anti bullying policy
- All incidents of online hate reported to the School will be reported
- All members of the School community will be advised to report online hate in accordance with relevant school policies and procedures
- The Police will be contacted if a criminal offence is suspected. If the School is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately from Durham Police

Appendix A

Permissible Use

	Staff & Adults					Pupils			
	Allowed	Allowed for selected staff	Allowed when children are not present	Allowed only in the Staff Room	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed
Devices can be handed in for secure storage	X					X			
Devices may be carried around the school			X						X
Devices may be turned on in school				X					X
Devices may be used in lessons					X				X
Devices may be used in social time				X					X
Cameras may be used on devices					X				X
Devices may use the school wireless network					X				X
Devices may be used to access social media					X				X
Use of school systems for personal use (e.g. E-mail, Shopping)					X				X

Acceptable User Actions (Children and Adults)

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Illegal and Unacceptable
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					x
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					x
	Pornography				x	
	Promotion of any type of discrimination				x	
	Threatening behaviour				x	
	Promotion of extremism or terrorism				x	
	Using school systems to run a business				x	
	Bypassing filtering systems				x	
	Infringing Copyright				x	
	Revealing or publishing personal data or network access information				x	
	Creating or propagating viruses or harmful files				x	

	Deliberately downloading files to limit internet usage by others				x	
	Online Gaming (Non-Educational)					
	Online Gaming (Educational)					
	Gambling					
	Shopping					
	File Sharing					
	Access to Social Media					
	Video Broadcasting e.g. uploading to YouTube					
	Use of YouTube (or other video site) (educational)					
	Use of YouTube (or other video site) (Non-educational)					

Pupil Incidents	Action / Sanction								
	Refer to Class Teacher / Tutor	Refer to Head	Refer to Police	Refer to Technical Support	Inform Parents	Removal of internet access rights	Confiscate Device and hand to parents	Warning	Further Action
Deliberately trying to access material which could be considered as illegal		x	x						
Use of a mobile device contrary to the school rules									
Use of non-educational sites during lessons									
Unauthorised use of Social Media during the school day									
Accessing another pupils account									
Allowing others to use your own account									
Attempting to access a staff account									
Sending a text or message which is deliberately hurtful									
Attempting to damage or destroy the work of others									
Attempting to bypass the filtering system									
Deliberately trying to access offensive or pornographic material									
Deliberately sending or receiving material which is in breach or copyright or data protection laws									

Staff Incidents	Action / Sanction								
	Refer to Line Manager	Refer to Head	Refer to Police	Refer to Technical Support	Refer to HR / LADO	Removal of internet access rights	Warning	Suspension	Further Action
Deliberately trying to access material which could be considered as illegal		x	x		x				
Use of a mobile device contrary to the school rules									
Inappropriate use of Social Media during the school day									
Careless misuse of data e.g. accidental use of non-encrypted memory sticks									
Deliberate misuse of data e.g. unauthorised use of cloud based storage systems									
Allowing others to use your own account									
Attempting to access an administrative account without permission									
Sending a text or message that that is regarded as offensive, harassment or of a bullying nature									
Attempting to bypass the filtering system									
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		x			x				

Actions which could compromise the staff member's professional standing and or bring the institution into disrepute									
Accidentally accessing offensive or pornographic material without reporting it									
Deliberately trying to access offensive or pornographic material									
Deliberately sending or receiving material which is in breach or copyright or data protection laws									

Appendix B

Questions to support DSLs responding to concerns relating to youth produced sexual imagery

The following statements may DSLs to consider how best to respond to concerns relating to youth produced sexual imagery:

Child/Young person involved

- What is the age of the child(ren) involved?
    - If under 13 then a consultation/referral to Children's Social Care should be considered.
    - If an adult (over 18) is involved, then police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- Is the child able to understand the implications of taking/sharing sexual imagery?
- Is the school or other agencies aware of any vulnerability for the children(s) involved? E.g. special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved? E.g. family situation, children at risk of sexual exploitation?
- Has the child(ren) involved been considered under KSCB 2.2.2 "children who display harmful behaviours" or the KSCB CSE toolkit?

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats or blackmail?
    - What was the intent for taking/sharing the imagery? E.g. was it a "joke" or are the children involved in a "relationship"?
        - If so, is the relationship age appropriate? For primary schools a referral to social care regarding under age sexual activity is likely to be required.
    - Is this behaviour age-appropriate experimentation, natural curiosity or is it possible exploitation?
- How were the school made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another pupil or member of the school community? If so, then how will the school safeguard the pupil concerned given that this is likely to be distressing to discuss.

- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?
- Is the imagery on a school device or a personal device? Is the device secured?
    - **NB: Schools and settings must NOT print/copy etc. imagery suspected to be indecent – the device should be secured until advice can be obtained.**

The Imagery

- What does the school know about the imagery? (Be aware it is unlikely to be necessary for staff to view the imagery)
    - Is the imagery potentially indecent (illegal) or is it "inappropriate"?
    - Does it contain nudity or sexual acts?
- Does the child(ren) know who has accessed the imagery?
    - Was it sent to a known peer (e.g. boyfriend or girlfriend) or an unknown adult?
- How widely has the imagery been shared? E.g. just to one other child privately, shared online publicly or sent to an unknown number of children/adults?

Action

- Does the child need immediate support and or protection?
    - What is the specific impact on the child?
    - What can the school put in place to support them?
- Is the imagery available online?
    - If so, have appropriate reports been made to service providers etc.?
- Are other schools/settings involved?
    - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
    - If so, what action was taken? **NB repeated issues will increase concerns for offending behaviour and vulnerability therefore an appropriate referral will be required.**

- Are the school child protection and safeguarding policies and practices being followed?
    - Is a member of the child protection team on hand and is their advice and support available?
- How will the school inform parents?
    - With older pupils it is likely that DSLs will work with the young person to support them to inform parents
- Can the school manage this issue internally or are other agencies required?
    - Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable pupils or risk of significant harm will always need involvement with other agencies.

Appendix C

Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It must not replace professional advice and schools and settings should always consult with their Area Safeguarding Adviser or the Education Safeguarding Adviser (Online Protection) from the Education Safeguarding Team, Legal representation, Local Authority Designated Officer or Police if they are concerned that an offence may have been committed.

Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a "higher law" which affects all other laws. Within an education context, human rights for schools and settings to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Schools and settings are obliged to respect these rights and freedoms, balancing them against rights, duties and obligations, which may arise from other relevant legislation.

Data protection and Computer Misuse

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, video and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, organisations have to follow a number of set procedures.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);

- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

The Protection of Freedoms Act 2012

This act requires schools to seek permission from a parent / carer to use Biometric systems.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Obscene and Offensive Content including Hate and Harassment

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send

a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

The Protection of Freedoms Act 2012 (2A and 4A) and Serious Crimes Act 2015 (section 76) - Stalking and Harassment

The Protection of Freedoms Act 2012 was updated in 2015 and two sections were added regarding online stalking and harassment, section 2A and 4A. Section 2A makes it offence for a perpetrator to pursue a course of conduct (2 or more incidents) described as "stalking behaviour" which amounts to harassment. Stalking behaviours include following, contacting/attempting to contact, publishing statements or material about the victim, monitoring the victim (including online), loitering in a public or private place, interfering with property, watching or spying. The Serious Crime Act 2015 Section 76 also created a new offence of controlling or coercive behaviour in intimate or familial relationships which will include online behaviour.

Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term "revenge porn" only apply to images or videos of those aged 18 or over. For more information access: www.revengepornhelpline.org.uk

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil "common law" tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance

of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. This act gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. The DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The School Information Regulations 2012

This act requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Sexual Offences

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

Section 15 - Meeting a child following sexual grooming. The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. This offence can result in imprisonment for up to 10 years.

Causing or inciting a child under 16 to watch or take part in a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 9. Sexual Activity with a child** (Can result in imprisonment for up to 14 years)
- **Section 10. Causing or inciting a child (13 to 16) to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 11. Engaging in sexual activity in the presence of a child** (Can result in imprisonment for up to 14 years)

- **Section 12. Causing a child to watch a sexual act** (Can result in imprisonment for up to 10 years)
- **Section 13. Child sex offences committed by children (offender is under 18)** (Can result in imprisonment for up to 5 years)

Section 16 - Abuse of position of trust: sexual activity with a child.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust and this can result in imprisonment for up to 5 years.

Indecent Images of Children

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom under two pieces of legislation; **Criminal Justice Act 1988**, section 160 and **Protection of Children Act 1978**, section 1.1.a. Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism.

A child for these purposes is considered to be anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This offence can include images taken by and distributed by the child themselves (often referred to as "Sexting", see section 9.1). Viewing an indecent image of a child on your computer or phone means that you have made a digital image and printing/forwarding/sharing/publishing can be considered to be distribution. A person convicted of such an offence may face up to 10 years in prison.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess "extreme pornographic images". 63 (6) identifies that such images must be considered to be "grossly offensive, disgusting or otherwise obscene". Section 63 (7) includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communication. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.

Appendix D

Online Safety Contacts and References

Durham Support and Guidance

Durham LA Safeguarding team

EDA with responsibility for online safety
Paul.Hodgkinson@durham.gov.uk
03000 265841
Pauline.Stewart@durham.gov.uk

Durham Police:
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Durham Police via 101

Information and advice on CSE
http://www.eraseabuse.org/

Durham Local Safeguarding Children Board (LSCB): http://www.durham-lscb.org.uk/

ICTSS - ICT Support for Durham Schools 03000 261100

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

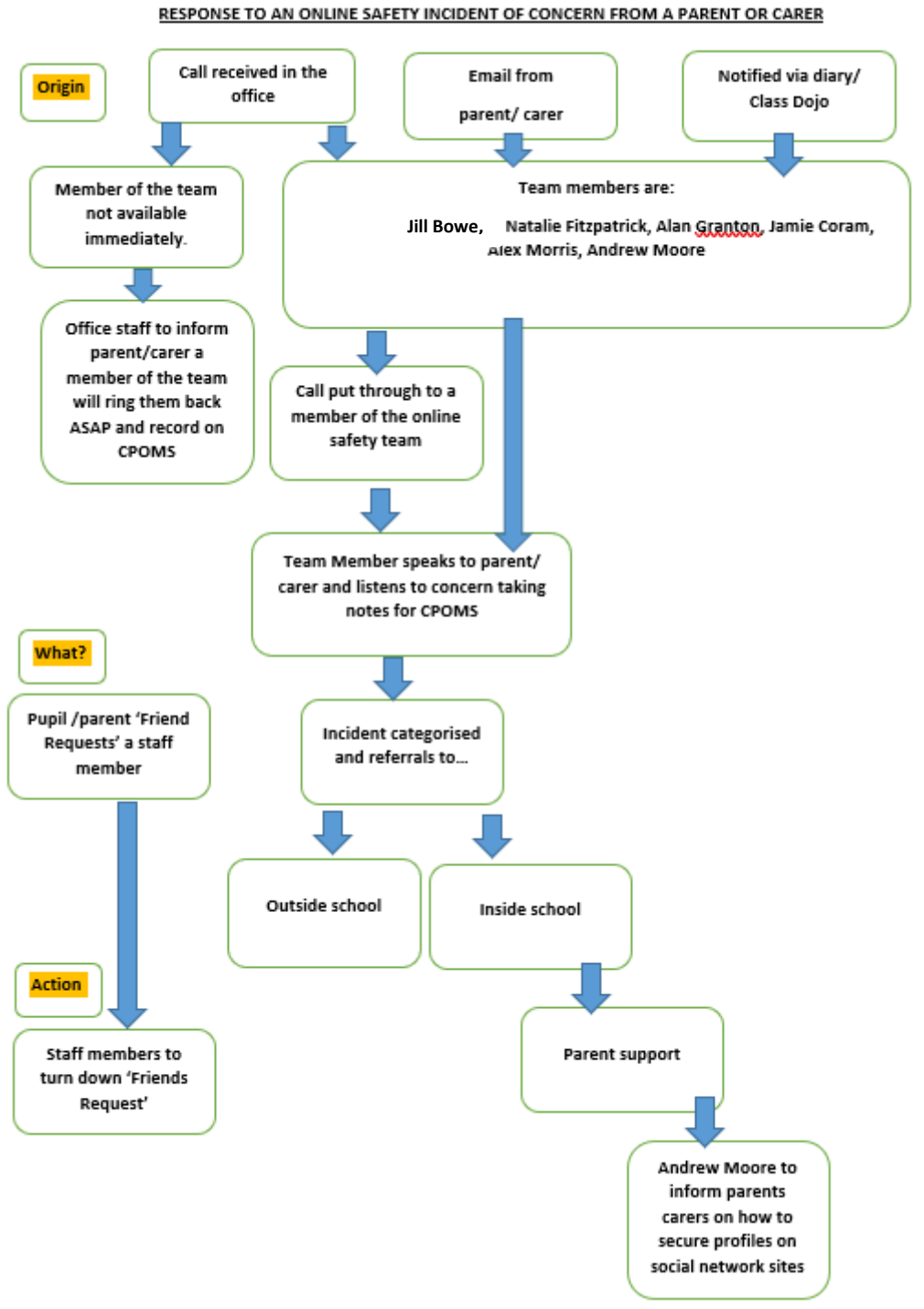
Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings):
http://www.onlinecompass.org.uk/

Appendix E


RESPONSE TO AN ONLINE SAFETY INCIDENT OF CONCERN FROM A PARENT OR CARER
Origin
Call received in the office
Email from parent/ carer
Notified via diary/ Class Dojo
Member of the team not available immediately.
Team members are:
Jill Bowe, Natalie Fitzpatrick, Alan Granton, Jamie Coram, Alex Morris, Andrew Moore
Office staff to inform parent/carer a member of the team will ring them back ASAP and record on CPOMS
Call put through to a member of the online safety team
Team Member speaks to parent/ carer and listens to concern taking notes for CPOMS
What?
Pupil /parent 'Friend Requests' a staff member
Incident categorised and referrals to...
Outside school
Inside school
Action
Staff members to turn down 'Friends Request'
Parent support
Andrew Moore to inform parents carers on how to secure profiles on social network sites

Appendix F

AI Update

At Villa Real School we follow the JCQ guidance on the use of AI, which states that "all work submitted for qualification or non-examined assessments (NEA's) must be the learners' own." This means ensuring that the learner's submission is their own work, and is not copied, paraphrased, or heavily derived from another source, including content produced by AI tools.

AI tools may be used appropriately as part of learners' work, provided that the final submissions are their own. This means both ensuring that the final product/outcome is in their own words and that the content reflects their own efforts. Learners are expected to demonstrate their own knowledge, skills and understanding as required for the qualification / NEA in question and set out in the qualification / NEA's specification. If learners use AI tools, it must be clearly referenced in their submissions.

A learner will have committed malpractice if they use AI tools without making appropriate references and in such a way that the work they submit is not their own. Where teachers have doubts about the authenticity of the work, they must investigate and take appropriate action.

When marking learner work that acknowledges AI use and demonstrates no misuse, teachers and assessors must ensure learners are not rewarded if they haven't independently met the marking criteria. Depending upon the marking criteria or grade descriptors, teachers or assessors may need to consider the failure to independently demonstrate understanding of certain aspects when determining the appropriate mark or grade.

Any staff member who identifies AI-based activities or software that is or may be in violation of the JCQ regulations must report the activity or software immediately to the Exams Officer. Any students / staff who are found to be in violation of the AI policy will be subject to disciplinary action as per the Villa Real School Malpractice Policy.