Vivid Mind Schools
E-Safety Policy

Date agreed by Governing Body: 19 June 2019

Date of next review: Summer term 2020

1. Policy Aims

This policy takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2016, Early Years and Foundation Stage 2017

The purpose of this policy is to:

- Safeguard and protect all members of our community.
- Identify approaches to educate and raise awareness of online safety throughout that community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Vivid Mind Schools identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

We believe that e-safety is an essential part of safeguarding and we acknowledge it is our duty to ensure that all pupils and staff are protected from potential harm online.

We confirm that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

We believe that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school

(collectively referred to as 'staff' in this policy) as well as pupils and parents/guardians.

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

2.2 Links with other policies and practices

This policy links with a number of other policies, practices and action plans including: o Anti-Harassment, Anti-Bullying Policy

o Code of Conduct for Staff Policy o Behaviour Management Policy

o Child Protection Policy o Confidentiality Policy
o ICT Security Policy

o Image Use Policy and Consent Form o ICT Teaching Policy
o Social Media Policy

3. Monitoring and Review

We will review this policy at least annually

- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure she has oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.

The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.

Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

The school has appointed Elen Peal, Patricia English and Katherine Mannion as Designated/ Deputy Safeguarding Leads to be the e-safety leads.

We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an Acceptable Use Policy (AUP), which covers acceptable use of technology. Ensure that suitable and appropriate filtering and monitoring systems are in place.

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

Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.

Support the Designated Safeguarding Leads by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.

Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.

Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.

Ensure all members of staff receive regular, up-to-date and appropriate online safety training.

Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

Ensure that online safety is promoted to parents, guardians and the wider community, through a variety of channels and approaches.

Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.

Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

Report online safety concerns, as appropriate, to the management team and Governing Body.

Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

Meet half termly with the governor with a lead responsibility for safeguarding.

4.3 It is the responsibility of all members of staff to:

Contribute to the development of online safety policies. Attend required e-safety training.

Read and adhere to the online safety policy and code of conduct.

Take responsibility for the security of school systems and the data they use, or have access to. Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

Embed online safety education in curriculum delivery, wherever possible – including assemblies. Have an awareness of a range of online safety issues and how they may be experienced by the
children in their care.
Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.

Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
Ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the leadership team.
Report any filtering breaches to the DSL and leadership team, as well as the school's Internet Service Provider or other services, as appropriate.
Ensure that any safeguarding concerns, identified through monitoring or filtering breaches, are reported to the DSL, in accordance with the school's safeguarding procedures.

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

Engage in age appropriate online safety education
opportunities. Respect the feelings and rights of others
both on and offline.

Take responsibility for keeping themselves and others safe online.

Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and guardians to:

Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.

Role model safe and appropriate use of technology and social media.

Abide by the school's home-school agreement and internet safety agreement. Identify changes in behaviour that could indicate that their child is at risk of harm online.

Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.

Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and how to validate information before accepting its accuracy.

The school will support pupils to understand their responsibilities by:

- Displaying acceptable use posters within the school.
- Informing pupils that network and internet use will be monitored for safety and security purposes
  and in accordance with legislation.
- Rewarding positive use of technology by pupils.
- Providing online safety education and training as part of the transition programme across the key
  stages and when moving between establishments.
- Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

5.1.1 Vulnerable Pupils

We are aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.

We will seek input from specialist staff as appropriate, including the SENDCO and Child in Care Lead.

5.2 Training and engagement with staff

The school will:

Provide and discuss the e-safety safety policy with all members of staff as part of induction.

Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.

Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.

Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school. Remind staff of their responsibilities on social media and WhatsApp groups etc. outside of school by referring them to the school's Social Media Policy (Appendix 8).

Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.

Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and guardians

We recognise that parents and guardians have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school will build a partnership approach to online safety with parents and guardians by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events.
- Drawing their attention to the school e-safety policy, Social Media Policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our school, for example, within our Acceptable Use Policy (Appendix 4).

6. Reducing Online Risks

We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.

- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

7. Safer Use of Technology

7.1 Classroom Use

We use a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras and video cameras
- All school-owned devices will be used in accordance with the school's expectations and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age-appropriate search tools.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and the source of information is acknowledged.

Supervision of pupils will be appropriate to their age and ability.

- **Early Years Foundation Stage and Key Stage 1**
  Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' ages and abilities.
- **Key Stage 2**
  Pupils will use age-appropriate search engines and online tools.
  Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' ages and abilities.

7.2 Managing Internet Access

All staff have access to the school's devices and systems. When a member of staff leaves, their access and email are removed.

Staff, governors and visitors are not permitted to use school wifi for personal devices. Use of wifi is restricted to school devices only.

An adult will always be in the room when children are using Internet-enabled devices, monitoring activity.

7.3 Filtering and Monitoring

7.3.1 Decision Making

Our governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.

The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.

The school's filtering and monitoring is supported by our IT consultants.

Our IT consultants ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

The school uses educational broadband connectivity through our IT consultants.

The school uses Surf Protect which blocks sites which can be categorised as pornography, racial hatred, extremism, gaming and sites of an illegal nature.

- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

The school works with our IT consultants/Surf Protect to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches:

- **Staff will follow the Responses flowchart (Appendix 2)**
- If **pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff.**
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/guardians will be informed of filtering breaches involving their child.

Any material that the school believes is illegal will be reported immediately to the appropriate agencies.

Responses Flowchart to be placed next to all fixed devices.

7.3.4 Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:

- *Reviewing logfile information for **internet and web access***

The school has a clear procedure for responding to concerns identified using the e-safety incident procedure. See Appendix 1.

All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with current Data Protection legislation.

- Full information can be found in the school's ICT Security Policy.

7.5 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including: o Updating Virus protection regularly.

- Encryption of personal data sent over the Internet or taken off site (such as via portable media storage), or providing access only via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.

From year *3* all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.

We require users to:

- o Use strong passwords for access into our system. o Change their passwords regularly (staff)
- o Always keep their password private; users must not share it with others or leave it where others can find it.
- o Not to login as another user at any time.
- o To log off/lock computer when leaving rooms.

7.6 Managing the Safety of the School Website

The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.

The administrator account for the school website will be secured with an appropriately strong password.

The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image Use Consent Form, ICT Security, AUPs, Codes of conduct, Social media.

7.8 Managing Email

Access to school email systems will always take place in accordance with Data Protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of Conduct.

- o The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- o Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- o School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the school community will immediately tell a member of the senior leadership team if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

7.8.1 Staff

The use of personal email addresses by staff for any official school business is not permitted.

- All members of staff are provided with a specific school email address to use for all official communication.
- School emails may be accessed via their personal mobile device as long as the device is password protected.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

Pupils will use school provided email accounts for educational purposes.

Pupils will receive education regarding safe and appropriate email etiquette before access is permitted.

Whole-class or group email addresses may be used for communication outside of the school

8.Use of Personal Devices and Mobile Phones

We recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/guardians, but technologies need to be used safely and appropriately within school.

8.1 Expectations

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour Management and Child Protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user at all times and the use or such devices is subject to the rules stated in points 8.2 to 8.5.

- All members of our community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.

All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour Management or Child Protection policies.

8.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or
  disabled during lesson times.
- Not use personal devices in front of pupils or during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and guardians on school matters.

- Any pre-existing relationships which could undermine this will be discussed with the
- In exceptional circumstances, the DSL may grant permission for direct contact to be made through such devices.

Staff will not use personal devices such as mobile phones, tablets or cameras:

- To take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Directly with pupils and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

8.3 Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

We expect that pupil's personal devices and mobile phones will be handed in at the school office at the beginning of the school day and collected at the end of the day. Parents must make a request to the school for their child to bring in the device and the Headteacher will consider if this request is appropriate and provide permission accordingly.

If a pupil breaches the school procedures the phone or device will be confiscated and held in a secure place.

8.4 Visitors' Use of Personal Devices and Mobile Phones

Parents, Volunteers, Governors helping in school should be focussing on the pupils. They must switch off their phones and not use them whilst on site. If a visitor needs access to their phone for an emergency they must request permission and a member of the senior leadership team will permit access if appropriate in specific designated areas.

Members of staff and governors are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Governors and visitors attending on school business (other than helping pupils or staff): phone calls or texts are acceptable only if they relate to school matters. They should request permission and use only in specific designated areas and not in the presence of pupils.

8.5 Officially provided devices .

Members of staff will be issued with a school email address.

School devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff and children, as directed by staff.

9. Responding to Online Safety Incidents and Concerns

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

All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns. See Appendix 1.

- Pupils, parents and staff are informed of the school's complaints procedure and staff are made aware of the whistleblowing procedure.

The school requires staff, parents, guardians and pupils to work in partnership to resolve online safety issues.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.

Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Thames Valley Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils' Welfare

The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL will record these issues in line with the school's Child Protection Policy.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Buckinghamshire Safeguarding Children Board thresholds and procedures.

The school will inform parents and guardians of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

Any complaint about staff misuse will be referred to the Headteacher, according to the Conduct & Discipline Policy.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local

Authority Designated Officer).

Appropriate action will be taken in accordance with the Behaviour Policy and Code of Conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

We recognise youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability-appropriate educational methods.

The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

If the school is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

- Act in accordance with our Child Protection and Safeguarding policies
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
  - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and guardians, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the school's Behaviour Policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with guidance.
  - Images will only be deleted once the school has confirmed that other agencies do not need to be involved and is sure that to do so would not place a child at risk or

    compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
  - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

We will ensure that all members of the community are aware of potential online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

We recognise online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/guardians.

The school will ensure that all members of the community are made aware of the support available regarding online child sexual abuse, both locally and nationally.

The school will ensure that the 'Click CEOP' report button is visible on the school website via the Safeguarding page and available to pupils and other members of the school community

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

If the school is made aware of an incident involving online sexual abuse of a child, the school will:

- Act in accordance with the school's Child Protection and Safeguarding Policy and Procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.
- Immediately inform the police via 101 (or 999 if a child is at immediate risk).
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/guardians about the incident and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; the school leadership team will review and update any management procedures, where necessary.

The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.

- Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/

If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the Police.

If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.

If pupils at other schools are believed to have been targeted, the school will seek support from the Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.

The school will take action to prevent accidental access to IIOC by using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Police and/or the Education Safeguarding Team.

If made aware of IIOC, the school will:

- Act in accordance with the school's Child Protection and Safeguarding Policy and procedures.
- Immediately notify the school's Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that 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, for example in emails, are deleted.
- Report concerns, as appropriate to parents and guardians.

If made aware that indecent images of children have been found on the school devices, the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that 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, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all

other copies) at the request of the police.
- Report concerns, as appropriate to parents and guardians.

If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:

- Ensure that the headteacher is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's Conduct & Discipline Policy.
- Quarantine any devices until Police advice has been sought.

11.4 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated.

Full details of how the school will respond to cyberbullying are set out in the Anti-Harassment, Anti-Bullying policy.

11.5 Online Hate

Online hate content, directed towards or posted by specific members of the community, will not be tolerated and will be responded to in line with existing school policies, including Anti-Harassment, Anti-Bullying and Behaviour.

All members of the 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 on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or the Police.

11.6 Online Radicalisation and Extremism

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child Protection Policy.

If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child Protection and Conduct & Discipline policies.

Appendix 1:

e-Safety Contacts and Resources

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

Action for Children: http://actionforchildren.org.uk/

Action Fraud: www.actionfraud.police.uk

Buckinghamshire Safeguarding Children Board: http://bucks-lscb.org.uk/e-safety

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

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/the-click-clever-click-safe-code-information-for-young-people

Digizen: www.digizen.org.uk

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

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

NSPCC: www.nspcc.org.uk/onlinesafety

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

Thames Valley Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries dial 101 or use http://www.thamesvalley.police.uk/

Think U Know website: www.thinkuknow.co.uk

UKCCIS UK Council for Child Internet Safety: https://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety

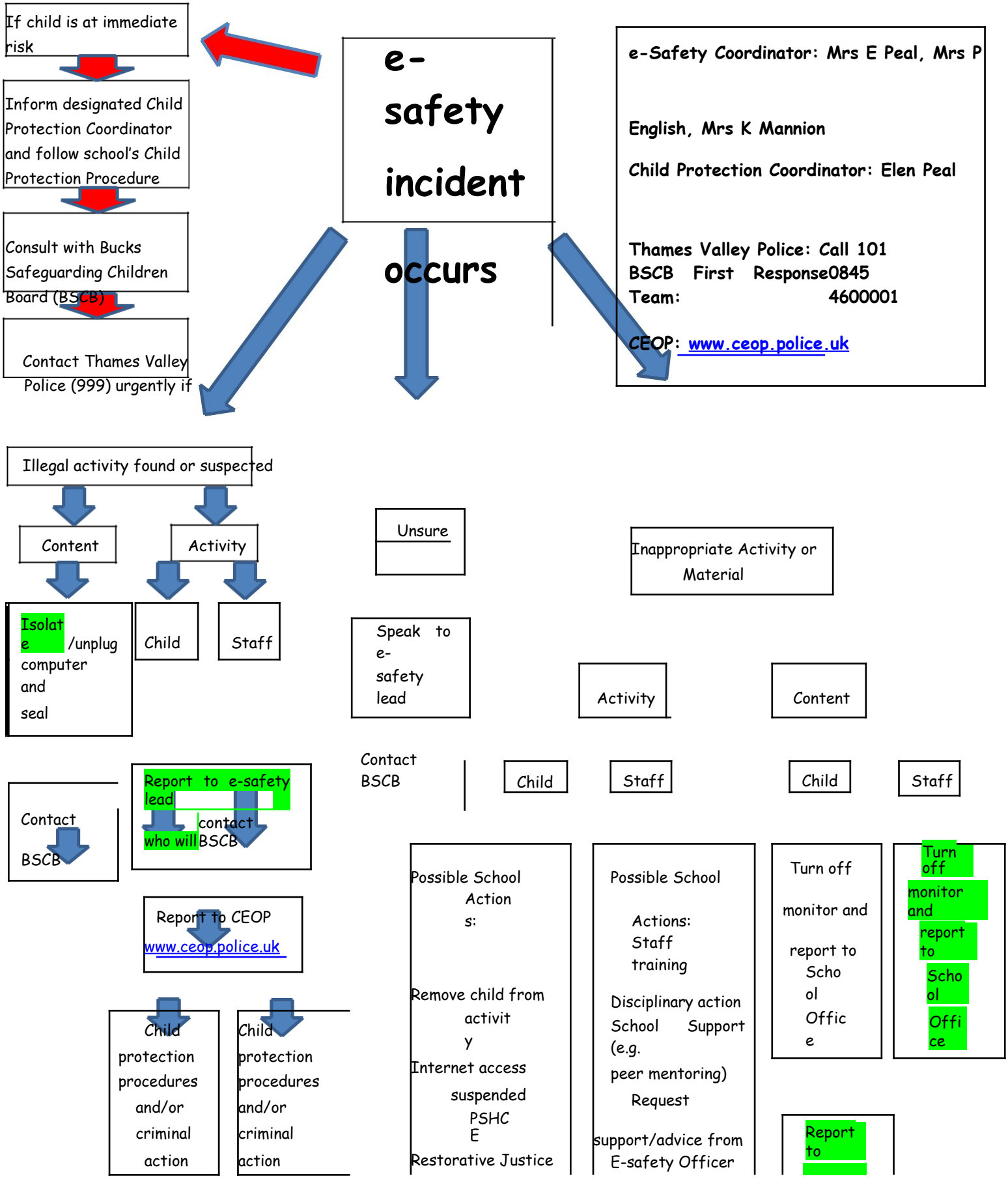
UK Safer Internet Centre: www.saferinternet.org.uk

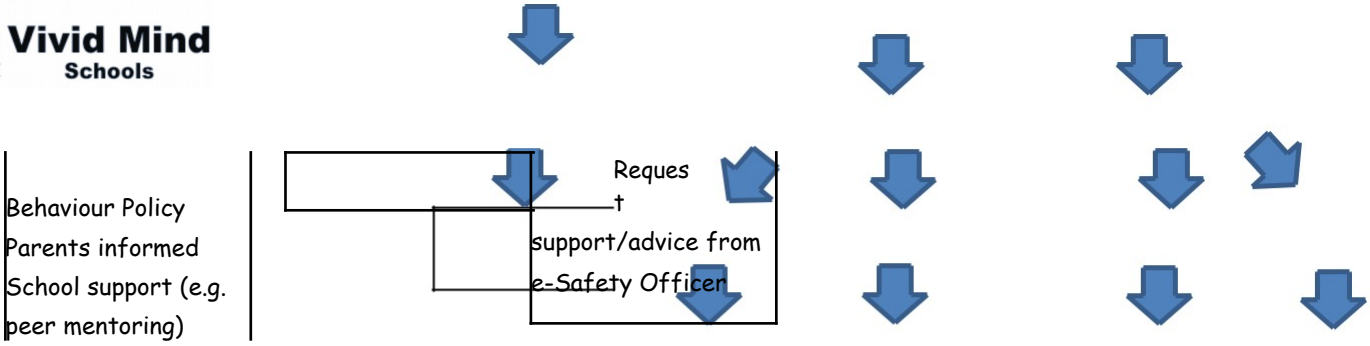
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Vivid Mind Schools

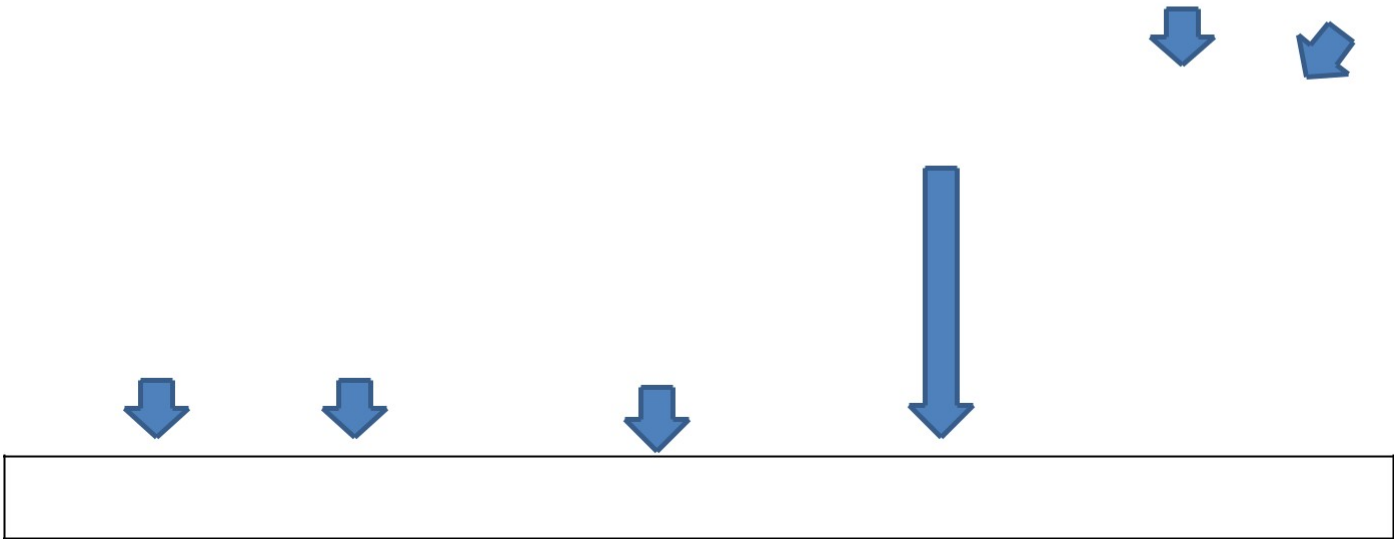
Appendix 2:

Response to an Incident of Concern





Review school's e-Safety policies and procedures, record actions in e-Safety Incident Log, implement any changes for the future



Appendix 3:

Vivid Mind Schools e-Safety Incident Log

Name of pupil or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

Appendix 4:

Vivid Mind School

Pupil Acceptable Use Policy – reviewed and agreed 20 February 2018

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

INTERNET:

I will only use the internet when supervised by a teacher or adult, or when given special permission. I understand that the school may monitor the web sites I have visited.

I understand that I can only access sites and materials relevant to my work in school.

I know that information on the internet may not always be reliable and sources may need to be checked.

I know that I will not be allowed to use the internet if I deliberately look at unsuitable material.

SECURITY & PRIVACY:

I will never tell anyone I meet on the internet my personal information or that of others (home address, telephone number, school's name) unless my teacher specifically gives me permission.

I will never send anyone my picture without permission from my teacher or parent/ carer. I will never give my password to anyone, even my best friend.

I will never arrange to meet anyone in person without first agreeing it with my teacher or parent/carer and I will get them to come along to the first meeting.

I will never hang around in an internet chat room if someone says or writes something which makes me feel uncomfortable or worried. I will always report it to my teacher or parent/carer.

I will never respond to unpleasant, suggestive or bullying emails, messages or bulletin boards. I will immediately report this to my teacher or parent/carer.

I will not look for bad language or distasteful images while I am online. I will report bad language or distasteful images to my teacher or parent/carer if I come across them accidentally.

I will always be myself and will not pretend to be anyone or anything I am not. I know that my teacher can see all the messages I sent through the VLE.

I will not take or distribute images of anyone without their permission.

I respect other people's work and will not access, copy, remove or change any other user's files without their knowledge and permission.

EMAIL:

I will be polite and responsible when I communicate with others

I know that posting of anonymous messages and forwarding of chain messages is not allowed. I will not use strong, aggressive, racist or inappropriate language.

I know that the contents of my email messages may be monitored by the school.

EQUIPMENT:

I will log off when I have finished using the computer.

I will not download or install software from the internet or attached to emails (including screen savers, games, video clips, audio clips, exe files) without permission.

I will not deliberately bypass any systems designed to keep us safer. I will not eat or drink near computer equipment.

I will look after all computer equipment and will report any loss or damage immediately, however this may have happened.

Vivid Mind School
Pupil Acceptable Use Agreement Form – reviewed and agreed 20 February 2018

This form relates to the CSG Village School Pupil Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP, discussed it with your child and agree to the rules included.

If any pupil does not comply with this Acceptable Use Policy (AUP), access to the school ICT systems will be suspended and the student will be subject to disciplinary action. Additional action may be taken in line with the existing positive behaviour policy. For serious violations, suspension or expulsion may be imposed. Where appropriate, the police may be involved or other legal action taken. For more information please see the schools e-Safety Policy.

Only once this agreement form has been signed and returned will access to the school ICT systems be permitted.

I have read and understood the above and agree to follow these guidelines when:

I use the school ICT systems and equipment

I use my own equipment out of school in a way that is related to me being a member of the school (e.g. communicating with other members of the school, accessing school e-mail, VLE, web site etc.)

Name of Pupil:

Parent/Carer Name:

Parent/Carer Signature:

Date: DD/MM/YYYY

APPENDIX 5:
Vivid Mind Schools
Staff, Governor & Volunteer Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

SECURITY & PRIVACY:

I understand that the school may monitor my use of the ICT systems, email and other digital communications.

I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.

I will respect system security and will use a strong' password. A strong password has numbers, letters and symbols, with 8 or more characters.

To prevent unauthorized access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

I will only use school wifi for school devices; I will not use it to access personal devices.

I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Headteacher.

I will not try to use any programmes or software or alter settings that might allow me to bypass the filtering or security systems in place.

I will not try to download, upload or access any materials which are illegal or inappropriate or may cause harm or distress to others.

I will only keep professional documents which contain school-related sensitive personal information on any devices that are secure and encrypted.

I will not use a personal camera or camera phone to record pupil images.

I will not publish any images of children outside the school environment without express permission from the parents and the Head teacher.

If offensive materials are found, I will immediately switch off the monitor, leave the computer running, confiscate any printed materials, CDs or memory sticks and report it to the Headteacher immediately.

I have read and understood the e-Safety policy which covers the requirements for safe ICT use.

If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Headteacher.

(EMAIL / INTERNET) COMMUNICATION:

I will access the internet for educational purposes only.

I will communicate with others in a professional manner; I will not use aggressive or inappropriate language.

I will only communicate with pupils, parents/guardians and other professionals via the approved communication

channels.

I will only respond to messages received from children relating to school matters. I will not open any attachments to emails, unless the source is known and trusted. I will not use personal email addresses on the school ICT systems.

Where work is protected by copyright, I will not download or distribute copies (including music and videos) unless permission has been granted.

I understand that disciplinary action may be taken if the internet is used inappropriately.

EQUIPMENT:

I understand that the rules set out in this agreement also apply to use of school ICT systems out of school (e.g. laptops, email, VLE). I will only use the school ICT systems for professional and educational purposes.

When I use personal portable media I will ensure they are protected by up-to-date virus software and are free from viruses.

I will not access, copy, remove or alter any other user's file, without prior permission.

I will not download or install software from the internet or attached to emails (including screen savers, games, exe files) without permission.

I will protect computer equipment from spillage by eating and drinking well away from them.

Vivid Mind Schools Staff, Governor & Volunteer Acceptable Use Agreement Form

This form relates to the Vivid Mind Schools Staff l Staff, Governor & Volunteer Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP.

I understand that if I fail to comply with this Acceptable Use Policy I could be subject to disciplinary action. I have read and understood the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff /Governor/ Volunteer:

Signature:

Date: DD/MM/YYYY

APPENDIX 6:
Vivid Mind School
e-Safety Audit

This self-audit should be completed annually by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher. Has the school an e-Safety Policy that complies with Bucks CC guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/guardians to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/guardians) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff (not just teaching staff)? Provide dates & details.	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment and annually thereafter?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/guardians or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/guardians and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider	Y/N

which complies with DfE requirements? Name:	
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N

Completed by (name and position): _____

Date : _____

APPENDIX 7:

External Photographers Contract

I understand the data protection considerations and am capable of meeting all responsibilities and obligations.

I shall only use the visual images for the purposes indicated by the school. Visual images shall be made available to the pupils or their parents only for personal use, either by the school itself or by the photographer. All images are stored safely and securely. All images will be deleted within a three year period of the date below. I will not have unsupervised access to children.

I have an up to date Disclosure and Barring Service (DBS) check which has been seen by the school.

Name:

Signature:

On behalf of CSG Village School:

Name:

Signature:

Date:

Appendix 8

Image Use Consent Form

To Name of the child's parent or guardian: _____

Name of child: _____

We take photographs of the children at our school. We may use these images in our schools prospectus, school blogs, or in other printed publications that we produce, as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

We need your permission before we can photograph or make any recordings of your child. Please answer questions 1-4 below, then sign and date the form where shown. **Please return the completed form to the school office as soon as possible.**

Please circle your answer

1. May we use your child's image in the school prospectus and other printed publications that we produce for promotional purposes? **Yes / No**
2. May we use your child's image on our website/blogs? **Yes / No**
3. May we use pictures of your child in images in and around the school that may be seen by visitors? **Yes / No**
4. May we use images of your child in the local media? **Yes / No**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please also note that the conditions for use of these photographs are on the back of this form.

I have read and understood the conditions of use on the back of this form.

Parent's or guardian's signature: _____ Date: _____

Name (in block capitals): _____

Conditions of use

1. This form is valid for the period of time your child attends Vivid Mind Schools, unless it is reviewed and amended within that time at which point you will be asked to sign the new version. The consent will automatically expire after this time.
2. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.
3. We will not use personal details or full names of any child or adult in a photographic image on video, on our website, in our school prospectus or in any other of our printed publications.
4. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.
5. If we name a pupil in the text we will not use a photograph of that child to accompany the article.
6. We may include pictures of pupils and teachers that have been drawn by the pupils.
7. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".
8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
9. For details about storage of media, please see our Privacy Notice, available on our website.