



# **Bromesberrow St Mary's C of E (VA)** **Primary School and Pre School**

**E-Safety/Acceptable User Policy**  
**October 2023**  
**Review: October 2024**

## **1. Guidance**

This policy applies to all members of Bromesberrow St Mary's C or E Primary School community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of Bromesberrow St Mary's C of E Primary School's digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this guidance, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The school will deal with such incidents within this guidance and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

The purpose of this Esafety Acceptable Use policy is to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that the school community has clear guidance on safe and acceptable use.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies both the school's and personal items that are brought into school if applicable.

## **2. Monitoring**

Bromesberrow St Mary's C of E Primary School will monitor the impact of this guidance by:

- Logging all reported incidents (CPOMs).
- DSL conducting a termly review of incident logs (Online folder)
- The DSL actioning preventative measures as needed (including but not limited to: providing extra lessons to effected year groups, collective worships and/or consulting outside agencies).
- The DSL commissioning a review into whether this extra teaching had the desired impact on children.
- Conducting surveys/questionnaires of children, parents/carers, and staff including nonteaching staff.
- The Co Headteacher's monitoring information about the teaching programme and coverage within the curriculum.
- The DSL regularly checking that children and staff are clear about how to report incidents and respond to them.
- Ensuring that the content of the website and Facebook account is regularly monitored by governors and senior leaders to ensure that it complies with this policy.

## **3. Roles and Responsibilities**

These are clearly detailed in Appendix 1 for all members of the Bromesberrow St Mary's C of E Primary School community.

## **4. Guidance Statements:**

### **4.1 Education of Children:**

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-safety is an essential part of Bromesberrow St Mary's C of E Primary School's e-safety provision.

Children and young people need the help and support to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum and staff should reinforce safety messages regularly. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced regularly to both staff and children when needed.
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Children should be helped to understand how to adopt safe and responsible use both within and outside of school.
- Staff should act as good role models in their use of digital technologies and the internet.
- Staff should check websites that children are using in ICT lessons and therefore ensure potential exposure to inappropriate material is minimised.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the children visit – this can also be addressed through Bromesberrow St Mary's C of E Primary School's network filtering capabilities. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study.

### **4.2 Children with SEND:**

The internet and technology are an integral part of everyday life for children. It is important that we acknowledge the positive opportunities the internet provides for children with Special Educational Needs and Disabilities (SEND); the accessibility of images and video online make it an excellent learning tool, whilst global connectivity enables children with SEND to socialise and access support. However, children with

SEND are more likely than their peers to experience online issues such as cyberbullying, online grooming and exploitation. Similarly, children with SEND are more likely to have their internet use restricted and therefore have limited opportunities to learn through experience, develop resilience or seek support, which would empower them to use technology safely.

E-safety is a fundamental part of our safeguarding responsibilities and at Bromesberrow St Mary's C of E Primary School we implement a range of targeted and differentiated strategies to enable children with SEND to access the internet safely and appropriately through:

- delivering e-safety education in an inclusive way, based on children's needs and experiences.
- building a collaborative understanding of the terminology being used.
- ensuring the 'rules' we provide are clear, consistent and not left open to interpretation.
- implementing a small step approach to online access, enabling children to develop experiences and build resilience in the online environment.
- using clear and accessible resources.
- providing a range of methods to enable children to report concerns and seek support.

#### **4.3 Education – Remote Education During School Closure:**

In the event of a Government mandated school closure during term time for a prolonged period, learning will need to continue remotely. This provision may be provided through providing live or recorded teaching input along with independent activities for children to complete. Teachers may rely on using pre-existing content online or creating their own and will therefore need to consider:

- Age appropriateness of the content being given.
- The possibility of the public being able to interact with a user.
- The possibility of inappropriate content being directly or indirectly (through advertisements etc.) accessed by the user.
- Data protection of the user's details. (see item 7).

Bromesberrow St Mary's C of E Primary School should look to use resources from websites that are already in use by school users and therefore where GDPR assessments have already been carried out, i.e. Tapestry, Teams, Purple Mash, Oak Academy, White Rose Maths and TT Rockstars.

Teachers may also wish to create their own original content such as video lessons or games, hosting directly onto Teams or Purple Mash which have been thoroughly explored and vetted, thereby avoiding third party websites/applications, which can mitigate risk of children inadvertently seeing undesired content. Using other sources would result in risk management being considered.

When recording content, teachers should be aware of their setting and any risk this carries. Recording in a room within the school building is the safest but this may not always be possible. Care should be taken if filming takes place in another location and teachers will need to make considerations such as:

- Choosing a suitable location – if at home, a garden, spare room or living room (not a bedroom) with a neutral background.
- Choosing suitable clothing.

- Being away from the general public.
- Ensuring the behaviour of anyone in their household does not compromise their content.
- Ensuring that any government-imposed restrictions on social distancing are adhered to.

#### **Interaction with Others:**

No website used by Bromesberrow St Mary's C of E Primary School currently allows the possibility of outside individuals knowingly interacting directly with children. Although, TT Rockstars does allow children to play with others around the world, there is no direct interaction, no real names are displayed and therefore it is impossible to know the identity of children as they are playing. Teams operates through direct invitation only. For live streaming lessons via Teams Bromesberrow St Mary's Primary School has ensured the safety of all its users by:

- Thorough research into platforms ahead of time with the advice of ICT providers and Government guidance where possible.
- Ensuring only the host can invite and grant access to users.
- Ensuring that no personal data of children is used, displayed or stored on the website – instead, an email and password is set up solely for Teams use.
- For those children who have photography restrictions in place, staff should communicate with parents in advance about the child attending online lessons using 'voice only' measures to remove any possibility of a photograph/screenshot of their child being attained.
- Parents to have agreed to children being able to access online learning through Teams platform prior to roll out.
- Children and parents to agree to have cameras on unless stated otherwise.
- Children to have an adult in the room whilst learning is taking place to support and help with any technical difficulties/ monitoring usage.
- Ensuring clear instructions to parents about language and expectations during the lesson.
- Ensuring clear instructions to children about expectations during the lesson – 'classroom standard' behaviour is still expected.

#### **4.4 Education – Parents/carers and the Wider Community:**

Some parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Bromesberrow St Mary's Primary C of E Primary School will therefore regularly update parents with information about keeping safe online through the following approaches. This will be the responsibility of the DSL (Leonie Mison):

- Curriculum activities
- Letters, newsletters, website.
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

#### **4.5 Education - Staff/Volunteers:**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this guidance. Training will be offered as follows:

- Staff will be updated of changes and updates to the E-Safety Guidance as part of a scheduled staff meeting when appropriate.
- All new staff should receive e-safety documentation as part of their induction programme, ensuring that they fully understand the school E-Safety Guidance and Acceptable Use Agreements. The DSL will liaise with the induction team about the materials that are to be shared.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety Guidance and its updates will be presented to and discussed by staff in staff meetings when necessary.
- The Co-Head teachers and DSL will provide advice/guidance/training to individuals as required.
- All staff will understand the need to report any harmful, illegal or inappropriate material (inc. radicalisation) to the DSL.

#### **4.6 Education – Governors:**

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/e-safety, safety/health and safety /safeguarding. This may be offered in the following ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in training provided by Bromesberrow St Mary's C of E Primary School/information sessions for staff or parents (this may include attendance at Assemblies/lessons).

### **5 Technical – infrastructure/equipment, filtering and monitoring:**

Bromesberrow St Mary's C of E Primary School will be responsible for ensuring that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this guidance are implemented through ensuring that The South West Grid for Learning 'filtered' Internet Service carries out all the online safety measures. It will also need to ensure that the relevant people named in Appendix 1 will be effective in carrying out their responsibilities. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the internet is dynamic in nature and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

We have robust systems in place for ensuring our filtering is effective. We have a filtering log, whereby we test and record our filtering systems regularly to ensure they are working. The Headteachers have direct access to the filtering system, so are able to access immediately if the need arises. This enables us to access reports on usage history when we need. Children are not left unsupervised when accessing the internet at Bromesberrow.

The technical role that Bromesberrow St Mary's C of E Primary School plays in maintaining the highest standards of safety are as follows:

- Bromesberrow St Mary's C of E Primary School's technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
  - There will be regular reviews and audits of the safety and security of school technical systems.
  - Servers, wireless systems and cabling must be securely located and physical access restricted.
  - All users will be provided with a username and secure password by the network manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
  - The IT Provider is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
  - Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider Integra. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
  - Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
  - An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person (DSL). Any incidents are to be logged in eSafety file on Safeguarding drive.
  - Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Bromesberrow St Mary's C of E Primary School's infrastructure and individual workstations are protected by up-to-date virus software.
- Staff and volunteers are aware of the current Esafety and Acceptable use policy.
  - Device User Agreements are in place regarding the extent of personal use that users and their family members are allowed on devices belonging to Bromesberrow St Mary's C of E Primary School that may be used out of school.
  - It is agreed when regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on Bromesberrow St Mary's Primary School C of E Primary School devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

All users have a responsibility to immediately report any infringements of Bromesberrow St Mary's C of E Primary School's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered. Staff have been granted a proxy service that can bypass filtering systems when needing to access resources they cannot – this should be used only on the occasion of accessing resources and is shared with co-head teachers.

## **5.1 Staff Passwords:**

All staff users will be provided with a username and password.

- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters. It must not include proper names or any other personal information about the user that might be known by others. They are not to be shared.

- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen and shall be securely hashed (use of one-way encryption).
- To minimise risk of data loss, passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the school.

## **5.2 Children's Passwords:**

All users will be provided with a username and password.

- Children will be taught the importance of password security.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

**General usernames and passwords for classes to access laptops also exist following this formula:**

Username - classname

Password – classname

## **Protection of Children's Usernames and Passwords:**

Children will have access to several usernames and logins alongside those used to access the Bromesberrow St Mary's Primary School C of E Primary School computer network for websites such as

TT Rockstars/NumBots, PurpleMash, Teams, Phonics Bugs (shared with children where appropriate) and others. Usernames and passwords should be pre-generated by school staff, who will keep a secure log of them if they need to be changed or access suspended.

Bromesberrow St Mary's C of E Primary School will give children individual access to logins so that no other person has access to them. Children will take usernames and passwords home through methods such as sticking them in the front of their reading records and taking them straight home. These can also be sent directly to parents if necessary. In the event a child feels someone else has gained access to their accounts, passwords can be changed at their request and to their choice. In events where this has happened, teachers should still be able to maintain administrative access to user accounts. Parents will be encouraged to communicate if they feel an issue has occurred and teachers will log any concerns.

## **6 Use of digital and video images:**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Bromesberrow St Mary's C of E Primary School will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm.



- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, such as on social networking sites.
- Written permission from parents or carers will be obtained before photographs of children are published on the Bromesberrow St Mary's C of E Primary School website/social media/local press. This process takes place as part of the induction consent obtained when children join the school.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images. All parents/carers are made aware of this.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must ensure images are stored on the school server and deleted immediately after use. They should only be shared and distributed in line with agreements gained from parents and to support educational aims.
- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the Bromesberrow St Mary's C of E Primary School website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's **full** names will **not** be used anywhere on a website or social media, particularly in association with photographs.
  - All staff have been provided with cameras to take photographs of children and have access to secure iPads, these will be used to take digital images/videos. Staff sign an agreement to not use personal devices in relation to digital images/videos.

## 7 Data Protection/GDPR:

According to the General Data Protection Regulation 2018, Personal data is information that relates to an identified or identifiable individual. If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

Personal data will be recorded, processed, transferred and made available according to the GDPR which states that personal data must:

- Not be kept for longer than is needed and be periodically reviewed, erased or anonymised if no longer needed.
- Bromesberrow St Mary's C of E Primary School should carefully consider any challenges to retention of data. Individuals have a right to erasure data if no longer needed (right to be forgotten).
- Personal data can be kept for longer if keeping it for public interest archiving, scientific or historical research, or statistical purposes.

## **7.1 Staff:**

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Transfer data using either encryption and secure password protected devices or, preferably, directly through the remote desktop service.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Do not use personal devices unless exceptional circumstance.

## **7.3 Remote Education:**

As mentioned in item 4.3, in the event of government-mandated school closures it will be necessary for children to have access to remote education that they can access from home. Teachers and leadership teams will therefore need to consider any GDPR implications this has.

Remote education provision should be designed using websites and providers that are already known to Bromesberrow St Mary’s C of E Primary School as much as possible. In these instances, GDPR checks and risk assessments will have already been carried out and usage is not likely to change requiring further assessment.

Username and passwords should be premade and given to children and carers ahead of time (see item 5.2). If content is being provided using other sources, teachers should ensure data protection regulations are being adhered to. For example:

- Content should be accessible without the need for children to provide personal information such as names, date of birth or address.
- Content should be hosted on reputable sites that do not expose users to unnecessary risk of dangerous pop-ups, viruses or hacking.
- Content should not require payment information to be given to be accessible.

## **8 Communications:**

When using communication technologies Bromesberrow St Mary’s C of E Primary School considers the following as good practice:

- The official Bromesberrow St Mary’s C of E Primary School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report communications that make them feel uncomfortable, are offensive, discriminatory, threatening or bullying in nature to their line manager, or DSL as appropriate. They must not directly respond to any such communication.
- Any digital communication between staff and children or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Bromesberrow St Mary’s C of E Primary School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Children should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with

inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the Bromesberrow St Mary's C of E Primary School website and only school email addresses should be used to identify members of staff.
- Staff are granted use of mobile phones on offsite visits and in the case of an emergency when the school phone is unable to be used. In the event of needing to contact a parent using own device, e.g. during a school closure, Headteachers have been informed and staff know their caller ID is not shown.

## **9 Social Media - Protecting Professional Identity:**

All schools, academies and local authorities have a duty of care to provide a safe learning environment for children and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees during their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Bromesberrow St Mary's C of E Primary School or the Local Authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Bromesberrow St Mary's C of E Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- Ensuring that personal information is not published.
- Training to include acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

Bromesberrow St Mary's C of E Primary School staff should ensure that:

- No reference is made on social media to children, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the Bromesberrow C of E Primary School community.
- Personal opinions are not be attributed to Bromesberrow St Mary's C of E Primary School or the Local Authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Personal use of social media within school is kept to a minimum. Where excessive personal use of social media within school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Bromesberrow St Mary's C of E Primary School's use of social media for professional purposes will be checked regularly by the Co Head teachers to ensure compliance with this E-Safety and acceptable use policy, and the Data Protection Policies.

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Bromesberrow St Mary's C of E Primary School. The school should effectively respond to social media comments made by others according to a defined policy or process.

### **9.1 Responding to incidents of misuse:**

This policy is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

## Illegal Incidents

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would be banned from the school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. If there is any suspicion that a website contains content that is highly inappropriate, or if there is any other suspected illegal activity, this should be logged in detail and all relevant members of staff be notified. Appropriate action should then be taken. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national/local organisations (as relevant)
  - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

Isolate the computer in question. Any change to its state may hinder a later police investigation. It is important that all the above steps are taken as they will provide an evidence trail for Bromesberrow St Mary's C of E Primary School and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. It is more likely that Bromesberrow St Mary's C of E Primary School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the school community are aware that incidents have

been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

## **Appendix 1 – Roles and Responsibilities**

### **Role Responsibility**

#### **Governors**

Governors are responsible for the approval of the E-Safety, acceptable use policy and for reviewing the effectiveness of this policy. This will be carried out by the Safeguarding Governor receiving regular information about online safety incidents from Bromesberrow St Mary's C of E Primary School's log of such incidents who will then report to the relevant Governors/Board

#### **Co Headteacher**

The Co Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the DSL

- The Co Headteacher and DSL and Deputy DSL should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (**see Appendix 2**).
- The Co Headteacher has a duty of care to ensure staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

**DSL** Should be trained in e-safety safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

The roles of the DSL are:

- To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing Bromesberrow St Mary's C of E Primary School's e-safety policies/documents.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- To provide training and advice for staff when needed.
- To liaise with the Local Authority/relevant body.
- To liaise with Bromesberrow St Mary's C of E Primary School's technical staff.
- To receive reports of e-safety incidents and use this information to inform future e-safety developments.

#### **Technical Lead-Integra**

Those with technical responsibilities (Forest IT) are responsible for:

- Ensuring that Bromesberrow St Mary's C of E Primary School's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that Bromesberrow C of E Primary School meets required e-safety technical requirements and any Local Authority or relevant body's online safety policy or guidance that applies to the setting.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy.

- Keeping up to date with e-safety technical information to effectively carry out their e-safety role and to inform and update others as relevant.
- Ensuring that the use of the network is monitored in order that any misuse/attempted misuse can be reported as detailed above.
- Monitoring of software/systems.

### **Teaching and support staff**

The teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current Bromesberrow St Mary's C of E Primary School E-Safety policy and practices.
- They have read and understood the E-safety and acceptable use policy.
- They report any suspected misuse or problems following the process within this document.
- All digital communications should be on a professional level and only carried out using official Bromesberrow St Mary's C of E Primary School systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Teaching, including remote education, ensures children understand and follow the E-Safety and Acceptable Use Policy.
- Teaching ensures children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (if applicable).
- In lessons where internet use is pre-planned, including signposting for remote education, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

### **Children**

Children are responsible for using Bromesberrow St Mary's C of E Primary School's digital technology systems in accordance with the Acceptable Use Policy.

They:

- Will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school.

### **Parents/ Carers**

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. Bromesberrow St Mary's C of E Primary School will take every opportunity to help parents understand these issues through:

- Parents' evenings
- Newsletter updates/letters
- Information about national/local e-safety campaigns and literature

Parents and carers will be encouraged to support the school in promoting good safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Live video call during a period of remote education
- This policy

Parents and carer will understand the need to report any harmful, illegal or inappropriate material (inc. radicalisation) to the appropriate member of the school.