Berkswell Church of England Primary School
Online Safety Policy - June 2020

Our Online Safety Policy has been written by the school, building on the SMBC Schools Online Safety Policy, SWGFL template policies and government guidance. It has been agreed by the senior management and approved by the governing body.

At the point of next review, it is planned that we will make consultations with the wider school community through a range of formal and informal meetings.

Schedule for Development / Monitoring and Review

The implementation of this policy will be monitored by:	Online safety coordinator (Mrs H Parker)
Monitoring will take place at regular intervals	Annually
The Governing Body will receive a report on the implementation of the Online Safety Policy (OSP) at regular intervals. (This may include anonymous details of online safety incidents)	Termly
The OSP will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date is	June 2021
Should serious online safety incidents take place, the following external persons / agencies should be informed.	LA safeguarding officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity/filtering
- Internal monitoring for network activity
- Surveys/questionnaires of
    - Pupils
    - Parents
    - staff

Purpose of Online Safety Policy

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to learners. The benefits are perceived to "outweigh the risks." However, schools must, through their online safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. Many of these risks reflect situations pupils meet in the off-line world and as such is intrinsically linked to many other school policies.

Scope of the Policy

This policy applies to all members of the Berkswell C of E School community, including staff, pupils, volunteers, parents, carers, visitors and community users who have access to and are users of the school ICT systems, both in and out of the school.

The Educations and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 online safety incidents covered by this policy, which may take place outside of the school but is linked to our community. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see Data Protection policy). In the case of both acts, action can only be taken over issues covered by the behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Governors

The School Governing body is responsible for the approval of the online safety Policy and fore reviewing its effectiveness. This is carried out at the full Governing Body Committee who receive regular information about online safety incidents. A member of the Governing Body has taken on the role of online safety Governor. The role of the Online Safety Governor will include:

- Regular meetings with the online safety coordinator
- Attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering logs
- Reporting to the relevant Governors meetings

Headteacher and Senior Leaders Leadership team

The Headteacher has a duty of care for ensuring the safety of members of the school community, though the day to day responsibility for online safety is delegated to the Online Safety coordinator.

The Headteacher and SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents Appendix 1).

The Headteacher and SLT is responsible for ensuring that the Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher/ SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net.

The SLT will receive regular monitoring reports from the Online Safety Leader.

Online Safety Leader

Our school Online Safety Leaders are responsible for keeping up to date on all online safety issues and ensuring that staff are updated as necessary. They are responsible for:

- Leading the Online Safety Group – to be developed
- Taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents.
- Ensuring that all staff are aware of the procedure that need to be followed in the event of an online safety incident
- Providing training and advice to staff
- Liaise with the LA when necessary
- Liaise with school technical staff
- Receive reports of online safety incidents and create a log of incidents to inform future online safety development
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering.
- Attends relevant meeting / committee of Governors
- Reports to the SLT

Network Manager / Technical support staff

The Network Manager and technical support staff (From SMBC) is responsible for ensuring:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets the required online safety technical requirements and Local Authority Online Safety guidance/policy that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Lead
- That monitoring software/systems are implemented and updated regularly.

School Staff

All staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of this policy and practices.
- They have read, understood and signed the Acceptable use agreement.
- They report and suspected misuse or problems to the Online Safety Coordinator for investigation/actions/sanctions.
- All digital communications with pupils or parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded within their teaching in all aspects of the curriculum.
- Pupils understand and follow the Online Safety policy and Acceptable Use Agreement.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable materials that is found in internet searches
- There is a culture where pupils feel able to report any bullying, abuse or inappropriate materials.

Designated Safeguarding Lead

The designated safeguarding leader should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Online Safety Group – to be developed

The online safety group will aim to provide a consultative group that has representation from the wider school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will aim to assist the Online Safety Leads with:

- The production / review / monitoring of the school Online Safety Policy / Documents
- Mapping and reviewing the online safety / digital literacy curricular provision – ensuring their relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents/carers and the pupils about the online safety provision
- Monitoring improvement actions identifies through the use of the 360 degree safe self-review tool

Pupils

Pupils:

- Are responsible for using the school digital technology systems in accordance with our Acceptable Use Agreement.
- Should have a developing understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the policies on the use of mobile devices and digital cameras. They should know and understand the policies on the taking of images and on online-bullying
- Should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that this policy covers their actions out of school, if related to their membership of it.
- Pupils know that their internet use in school is monitored.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents will be able to access the school's Online Safety policy on request. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents as appropriate. From time to time, parents will be provided with additional information on online safety in the form of written communication or workshop type events. This maybe in conjunction with the other schools in the rural collaborative. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school.

Other Community Users

There are very few community users who access the school systems, however, they are expected to sign an Acceptable Use Agreement before being provided with access to the school systems.

Education: Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating our pupils to take a responsible approach. The education of our pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be in the following ways:

- A planned online safety curriculum is provided as part of computing and PSHE and are regularly visited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials they access online.
- Pupils are taught that they need to acknowledge the source of information used and respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating difficult issues and helping the to understand how they can influence and participate in decision making.
- Pupils are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is planned, it is best practice for pupils to 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.
- When pupils need to freely search the internet as part of their lesson, staff are vigilant in monitoring the content of the websites they visit.

Education: Parents and Carers

Many parents have a limited understanding of online safety risks and issues, yet they play an essential role in their education of their children and in the monitoring/regulation of their children's online 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.

The school therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,
- Sharing useful publications through Twitter
- Events e.g. Safer Internet Day
- Reference to relevant websites/publications.

Education: Staff/Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- We are beginning to develop a programme of online safety training which will be made available to staff. When this is up and running, it will be regularly updated and reinforced. An audit of online safety training needs of staff will be carried out.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

- The Online Safety Leader will receive updates through attendance at external training events e.g. from the LA and be reviewing guidance documents released by relevant organisations.
- The Online Safety Policy and it's updates will be presented to and discussed by staff in team meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required

Training – Governors

Governors should take part in online safety training/awareness sessions.

Technical – infrastructure/equipment, filtering and monitoring

The school works in partnership with Solihull MBC and Becta to ensure filtering systems to protect pupils are reviewed and improved regularly although it remains the responsibility of the school to ensure that the managed service provider carries out all the online safety measures. It is important that the technician is fully aware of the school's Online Safety Policy and Acceptable Use Agreements.
The School is responsible for ensuring that the school's infrastructure/network is as safe and secure as it is reasonably possible and that policies / procedures approved within this policy are implemented. It will also ensure that the relevant people are effective in carrying out their online safety responsibilities.

- The school technical systems are 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 the school's technical systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to the school technical systems and devices.
- All users (KS1 and above) are provided with a username and secure password. Users are responsible for the security of their username and password. (Pupils in KS1 understand that their teachers may know these so that they can be supported when learning to logon to the system)
- Internet access is filtered for all users. The school has differentiated user level filtering for different levels of user.
- Internet filtering should ensure that our pupils are safe from terrorist and extreme material when accessing the internet.
- Technical staff regularly monitor and record activity of users on the school's technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school's systems and data. This is managed by SMBC technical staff and are tested regularly. The school infrastructure and individual work stations are protected by up to date virus software.
- Personal data cannot be sent over the internet or take off the school site unless safely encrypted or otherwise secured.

Using the Internet and digital communications for learning

New technologies have become an integral part of the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information technologies are powerful tools, which open up new opportunities.

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. Using the Internet for learning is now a part of the National Curriculum for Computing. We teach all of our pupils how to find appropriate information on the Internet, and how to ensure, as far as possible, that they understand who has made this information available, and how accurate and truthful it is.

• Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
• Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
• They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
• They are taught how to carry out simple checks for bias and misinformation
• They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Mobile Technologies

Mobile technology devices may be provided by the school or personally owned by staff and might include: smartphone, tablet, notebook / laptop or other technology that has the capacity to utilise our school wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users understand that the primary purpose of the use of these devices in school is educational. The mobile technologies policy is consistent with and inter-related to other school policies including: Safeguarding policy, Behaviour policy, Anti-bullying policy and Acceptable Use policy. Teaching about the safe and appropriate use of mobile technologies is an integral part of our Online Safety Teaching Programme.

The school allows the use of school owned devices during lesson time. Personal devices owned by the staff are only to be used during break times (see mobile phone policy). Pupils are not permitted to bring their own devices except in exceptional cases which are agreed with the Headteacher.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils 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 e.g. on social networking sites.
- Written permission from parents/carers is obtained before photographs of pupils are published in the school website/Twitter account/local press.
- 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 in not covered by the Data Protection Act).
- Staff are allowed to take digital / Video images to support education aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without permission
- Photographs published in the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school will ensure that:

- It has a data protection policy
- It has paid the appropriate fee to the Information Commissioner's Officer
- It has appointed a Data Protection Officer
- It will hold a minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Data held must be accurate and up to date. Inaccuracies are corrected without delay
- The lawful basis for processing personal date has been identified and documented and detailed in a privacy notice
- Where special category data is processed, a lawful basis and separate condition for processing have been identified
- Data Protection Impact Assessments are carried out
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Request to see all or part of their personal data held by the data controller

- There are clear and understood data retention policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- It has a Freedom of Information Policy which sets out how it deals with FOI requests
- All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of it's loss or misuse at all times
- 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
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with the school policy once it has been transferred or it's use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefits of using these technologies for educational purposes:

Communication Technologies	Staff	Pupils
Mobile phones may be brought to school	Allowed	Not allowed except in exceptional circumstances agreed by the Headteacher/ Class Teacher
Use of mobile phones in lessons	Not allowed	Not allowed
Use of mobile phones in social times	Allowed – where there are no pupils present	Not allowed
Taking photos on mobile phones	Not allowed	Not allowed
Use of other mobile devices (iPads, school owned tablets)	Allowed	Allowed
Use of personal email addresses in school or on school network	Allowed – where there are no pupils present	Not allowed
Use of school email for personal emails	Allowed	Allowed
Use of messaging Apps	In own time	Not allowed
Use of Social media	Use of school Twitter account in lesson time Personal accounts – in own time	Not allowed
Use of blogs (Seesaw)	Allowed	Allowed as directed

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users, including pupils, should be aware that email communication is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with this policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, etc) must be professional in tone and content. These communications should only take place on official (monitored) school systems.
- Email is not used with KS1 pupils, while pupils at KS2 are taught how to access individual email addresses for educational use.

- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and are frequently reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the school website and only official email addresses are used to identify members of staff.

Social Media – Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. The school or LA could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or LA liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

We provide the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use, social media risks, checking of settings, data protection, reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff ensure that:

- No reference is made in social media to pupils, parents/carers or staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or LA
- Security settings on personal social media profiles are regularly checked to minimise the loss of personal information

Personal use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary actions may be taken.
- The school permits reasonable and appropriate access to private social media sites.

The school's use of social media for professional purposes will be checked regularly by the Online Safety Lead and Online Safety Group to ensure compliance with school policies

Responding to incidents of misuse

Illegal incidents

See Appendix

Other Incidents

It is hoped that all members of the Berkswell school community will be responsible users of digital technology, who understand and follow our policy. However there may be times when infringements of the policy could take place, through careless or irresponsible or, rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have one or more members of the SLT involved. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using the same designated computer that will not be used by young people and if necessary can be take off site by the police should the need arise.
- It is important to ensure that the relevant staff should have appropriate access to the internet 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 the site containing the alleged misuse and describe the nature of the content causing concern. It may 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 cases of images of child sexual abuse).

- Once this has been completed and fully investigated the group will need to judge whether the concern has substance or not. If it does then appropriate action will be required. This may include:
    - Internal response or disciplinary procedures
    - Involvement by the LA
    - Police involvement/action
- **If content being reviewed includes images of child sexual abuse then 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 images to a child
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials
- **Isolate the computer in question. Any change to it's state could hinder a later police investigation.**

It is important to follow the correct procedure as this will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Berkswell School Actions and Sanctions

It is more than likely that we 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 procedures as follows:

Managing Internet Access and security

The school will maintain a current record of all staff and pupils who are granted Internet access. All users must read, sign and abide by the 'Responsible ICT Use Policy' before using any school ICT resource. At the Foundation Stage and Key Stage 1, access to the Internet will be by directly supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form for pupil access.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly check to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and antispam protection.
- Access to school networks for all users will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help identify patterns of behaviour and to inform the Online safety policy.
- The security of the school IT systems will be reviewed regularly.

Managing Internet use

Our school will provide an age appropriate Online safety curriculum (see PSHE Curriculum maps) that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Online safety is also an integral part of the computing curriculum and is linked to all lessons which are internet based.

Any, and all, communication between staff and pupils or families will take place using school equipment and/or school accounts. Pupils will be advised not to give out personal details which might identify them or their location.

Publishing images of staff and children

Photographs on the school website or Twitter that include pupils will be selected carefully. Names will not be used anywhere on the website or on Twitter (from June 2020), particularly in association with photographs. Written permission from parents or carers is obtained before photographs of pupils are published on the school website or Twitter.

Images of staff are not be published without consent.

Managing Email

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and risk assessments will be carried out before use in school is allowed.

- Mobile phones and associated cameras will not be used in lessons of formal times in line with our mobile phone policy.
- Games machines including Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering and cannot be used in school.

Use of personal devices

- Personal equipment should not be used by staff to access the school IT systems.
- Staff must not store images of pupils or pupil personal data on personal devices.
- Pupils are discouraged from bringing personal devices to school (mobile phones, tablets, SMART watches etc) however, we do recognise that in some exceptional circumstances children will need to do this. If they do, the devices will be securely stored by the class teacher and returned at the end of the day. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Managing Information Services

The security of the school information systems will be reviewed regularly.
Virus protection will be updated regularly and security strategies will follow Solihull MBC guidelines.
Portable media may not be used without specific permission followed by a virus check. Where they are used to store personal information they will be encrypted.

Data Protection

Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer that is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school will ensure that:

- It will hold the minimum of personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy notice" and lawfully processed in accordance with the Conditions for Processing. (see privacy notice)
- It has a data protection policy
- It is registered as a data controller for the purpose of the Data Protection Act.

Staff ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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.
- Transfer data using encryption and secure password protected devices.

Social networking

Social networking sites and newsgroups will be locked on the school networks unless a specific need is approved. Each of the following points are discussed with the children so that they understand them:

1. Never post any personal information (such as age, hobbies, phone numbers, where they live, photographs etc).

2. Never post anything that you would find upsetting (bullied/bullying).

3. If you find anything upsetting, don't reply, tell an adult you trust.

4. Be careful who you talk to, not everybody is who they say they are.

5. If somebody asks you to meet them in the real world, tell your parents or an adult.

Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. Pupils are taught about the consequences of cyberbullying and how it fits specifically into the school's antibullying ethos and policy.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Cyber-Bullying

Cyber-Bullying consists of: threats and intimidation sent to a pupil by mobile phone, email or online; harassment through repeated unwanted contact of another person; name calling online; pupil posting or forwarding of images without consent. Allegations of cyber-bullying will be handled in the same way as bullying. (Ref: anti-bullying policy)

Sexting

Whilst there is no clear definition of 'sexting', many professionals consider this to be 'sending or posting sexually explicit images including nude or semi-nude photographs, via mobiles or over the internet' whilst many children believe it to be 'writing and sharing explicit images with people they know'. Similarly, many parents think of sexting as 'flirty or sexual text messages' rather than images.

Sharing photos and videos online has become a part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. These can be shared as texts, emails, on social media and via messaging apps e.g. WhatsAPP or Snapchat. The increase in speed and ease of sharing imagery has brought concerns about young people producing and sharing images of themselves and although the production of such imagery will likely take place outside of school, the issues surrounding them often manifest during school time. Our school needs to be able to respond quickly and confidently to ensure that any affected pupil is safeguarded, supported and educated.

First and foremost, should an incident of sexting occur, we will respond in line with the schools safeguarding and child protection procedures. (Ref Safeguarding and child protection Policy)

Educating our pupils about the risk of Sexting

Learning about youth produced sexual imagery cannot be taught in isolation and as such it is intrinsically linked with our PSD curriculum as well as our computing schemes of work which in themselves link to the current National Curriculum programmes of study.

Given the sensitivity of these lessons we take great care to ensure that this issue is taught within an emotionally safe classroom climate where ground rules have been clearly established.

All teaching and learning around this issue is both age and readiness appropriate and is taught in a balanced and relevant way.

Prevent Duty (July 2015 update)

- Suitable filtering and supervision should be in place in order to ensure children are kept safe from terrorist and extremist material when accessing the internet in school – *Ref: Prevent Policy*
- Through Online safety and PSD lessons, pupils are to be equipped with the skills and knowledge necessary to stay safe from inappropriate material online, including terrorist and extremist material.
- Every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.
- Fundamental Christian and British values are advertised and delivered to the children on a regular and embedded basis, within the wider school curriculum.

Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither can the school or SMBC accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT use to establish if the Online safety policy is appropriate and effective.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

1. Making a note of the website and any other websites linked to it.

2. Informing the ICT Administrator.

3. Logging the incident.

4. Discussion with the pupil about the incident, and how to avoid similar experiences in future.

Handling Online safety complaints

- Formal complaints of Internet misuse will be dealt with by a senior member of staff. (Ref: Behaviour policy)
- Any complaint about staff misuse must be referred to the head teacher who should use the agreed SMBC procedures.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of the consequences for pupils misusing the internet. (Ref Behaviour policy)

Policy Review

- This policy will be reviewed annually and updated in line with the DfE or SMBC guidance or legislation.

Appendix 2

The role of the Online safety coordinator.

- Complete an annual Online safety audit in conjunction with the Senior Leadership Team and/or Head.
- Promote a culture of Online safety under the direction of the leadership team, and promote the school's e-safety vision to all stakeholders.
- Maintain the school's e-safety policy, reviewing annually.
- Ensure that the e-safety policy links with other appropriate policies e.g. Anti-Bullying, Child Protection, Computing, PSD etc (with the appropriate member of staff).
- Ensure the e-safety policy and its associated practices are adhered to.
- Ensure the Responsible use policies / school internet rules are in place, up to date and wherever possible are agreed by Staff, Pupils and Parents.
- Work with the SENCo and Designated Child Protection Officer to create e-safety guidance for vulnerable children and those with additional learning needs where appropriate.
- Manage e-safety training for all staff and ensure that e-safety is embedded within the culture of the school.
- Ensure staff receive relevant information about emerging issues.
- Coordinate e-safety awareness raising / education for pupils and ensure that e-safety is embedded into the curriculum, for example the computing schemes of work, worships and/or theme days.
- Support e-safety awareness raising/education initiatives for parents.
- Act as a point of contact, support and advice on e-safety issues for staff, pupils and parents.
- Act as a first point of contact should an e-safety incident occur and ensure that the e-safety procedure is followed, as outlined in this policy.
- Maintain an e-safety incident log in collaboration with the schools' safeguarding procedures.
- Monitor, report and address incidences of pupils accessing unsuitable sites at school as necessary.
- Keep up to date with local and national e-safety awareness campaigns and issues surrounding existing, new and emerging technologies.
- Work with and receive support and advice from SMBC.