Berkswell Church of England Primary School
E-Safety Policy- February 2017

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

Purpose of E-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 e-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 anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

E-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.

Leadership team

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures.

E-Safety Co-ordinator

Our school e-Safety Co-ordinator is responsible for keeping up to date on all e-Safety issues and ensuring that staff are updated as necessary. (Further details of their role are in Appendix 1)

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy. This is carried out at ******* committee who receive regular information about online safety incidents. A member of the Governing Body has taken on the role of Online Safety Governor.

Headteacher

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 E-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).

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

E-Safety Coordinator

See Appendix 1

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 requires 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 the network is regularly monitored in order that any misuse/ attempted misuse can be reported to the Headteacher.
- 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 Responsible use agreement.
- They report and suspected misuse or problems to the E-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.
- Pupils understand and follow the E-Safety policy and Responsible Use Agreement.
- They promote and support safe behaviours in their classrooms and following school e-Safety procedures.
- There is a culture where pupils feel able to report any bullying, abuse or inappropriate materials..

Pupils

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Responsible 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 cyberbullying
- 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 e-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 e-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

Community users who access the school systems will be expected to sign a Responsible 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 Responsible Use Agreement and encouraged to adopt safe and responsible use both withing 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 ther 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,
- Parents/carers evening sessions
- 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:

- A programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- 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 Responsible Use Agreements.

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. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school e-Safety coordinator. A designated senior leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. We will ensure that:

- The school technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There will 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 reposonsible 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.
- 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.
- 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 ICT 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.

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 e-safety policy.
- The security of the school IT systems will be reviewed regularly.

Managing Internet use

Our school will provide an age appropriate e-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. E-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. Full names will not be used anywhere on the website or on Twitter, particularly in association with photographs. Written permission from parents or carers will be 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.

Teachers have access to 'You Tube,' in school to support the curriculum and learning, all material must be vetted prior to use.

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 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 daya 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, 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 e-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 e-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 e-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.

Agreed by the Governing Body on:

Next review: Spring Term 2018

Appendix

The role of the e-safety coordinator.

- Complete an annual e-safety audit in conjunction with the Senior Leadership Team and/or Head.
- Promote a culture of e-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.

Extract from SWGfL Online Safety

Responding to incidents of misuse – flow chart