KINGSHILL CHURCH SCHOOL

BATH & WELLS
Multi Academy Trust
'That they may have life, life in all its fullness' John 10:10

E-SAFETY POLICY

Sep 2016

Rationale

New technologies have become integral to 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 and information technologies are powerful tools which open up opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The use of these tools in school and at home has been shown to raise educational standards and promote pupil achievement. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school e-safety policy helps to ensure safe and appropriate use (see also the school's Safeguarding and Child Protection Policy). However, the use of these technologies can put young people at risk within and outside the school. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with Kingshill Church School's behaviour, anti-bullying, safeguarding and child protection policies. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of our school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers the Headteacher, 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 e-safety incidents covered by this policy which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and within the anti-bullying policy and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Monitoring and Review of this Policy

The implementation of this e-safety policy will be monitored and reviewed by the Designated Teacher(s) for Safeguarding in consultation with the E-Safety Governor Headteacher and reviewed by the Local Governing Board (LGB).

The E-safety Governor will report to the Local Governing Board on the implementation of this policy at least annually. The E-safety policy will also be reviewed annually, or more frequently in light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

The policy will be monitored through:-

- Logs of reported incidents
- Exa network monitoring logs of internet activity (Exa networks currently provides the school's filter system)
- Surveys and questionnaires of pupils, parents/carers and staff.
- E-safety Committee meetings

Roles & Responsibilities

Roles	Responsibility
Governing Board	● Approval of the E-Safety Policy and for reviewing its effectiveness annually. ● Appointment of E-Safety Governor, whose role will include: ° Meetings as required with the Designated Teacher(s) for Safeguarding ° Annual or as necessary, monitoring of e-safety incident logs ° Annual or as necessary, monitoring of filtering / change control logs ° Reporting to full Local Governing Board
Head teacher, Senior Leadership Team & Designated Teacher(s) for Safeguarding	● The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibility for E-Safety will be delegated to the Designated Teacher(s) for Safeguarding ● The Headteacher and SLT are responsible for ensuring that the Designated Leads for Safeguarding and other relevant staff receive appropriate CPD to enable them to carry out their roles and to train other colleagues as required ● The Headteacher and the SLT will ensure that there is a system in place to allow for monitoring and support for those in school who carry out the internal e-safety monitoring role

	● The Headteacher and the SLT will receive regular monitoring reports (no more than termly) from the Designated Teacher(s) for Safeguarding ● The Headteacher and another member of the SLT will be aware of the procedures to follow in the event of a serious e-safety allegation being made against a member of staff ● The Headteacher and Designated Leads for Safeguarding will ensure that any action taken is in line with the other related policies

Roles	Responsibility
Designated Leads for Safeguarding	● Takes day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school's e-safety policies and procedures ● Ensures that all members of staff are aware of the procedures to follow in the event of an e-safety incident taking place ● Liaises with external bodies ● Liaises with the school's ICT technical staff ● Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments ● Meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering/change logs ● Attends relevant meetings, including LGB meetings as appropriate ● Reports regularly to the SLT

Roles	Responsibility
Teaching and Support Staff	Are responsible for ensuring that: ● They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices ● They have read and understood and signed the school's Staff Acceptable User Policy (AUP) at least annually or as required ● They report any suspected misuse or problem to the Designated Teacher(s) for Safeguarding for investigation/action/sanction ● Digital communications with pupils should be on a professional basis only and are only via the official school systems; ● E-safety issues are embedded in all aspects of the curriculum and other school activities;

	● The school's E-safety and Acceptable Use Policy is shared and understood by learners ● Pupils have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations ● They monitor ICT activity in lessons, extra-curricular and extended school activities ● They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school 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 material that is found in internet searches ● Their participation in any forum does not breach confidentiality or cause reputational damage to the school (exercise anonymity) ● Their use of ICT does not contravene the Data Protection Act or breach the school's Confidentiality Policy. ● Any documents/equipment/media taken off site are stored safely and securely, and in accordance with school procedures. ● Staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher and the ICT technician
Designated Lead for Safeguarding & Child Protection	Should be trained in e-safety issues and be aware of the potential for serious 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; ● Cyber-bullying
E-safety Committee	Comprising staff, pupils and governors ● report on day to day E safety issues ● monitor E-safety ● plan for E- safety week

Roles	Responsibility
Pupils	Have a responsibility to: ● Use the school's ICT systems in accordance with the appropriate Pupil Acceptable Use Policy which they will be expected to sign before being given access to school systems ● Have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations

	● Understand the importance of, and the procedures for, reporting incidents of abuse, misuse or access to inappropriate materials ● Know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images, and on cyber-bullying ● Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school
Parents/Carers	Parents/Carers play a crucial role in ensuring that their child(ren) understands the need to use the internet/mobile devices in an appropriate way. Research shows that many parents/carers do not fully understand the issues and are less experienced in the use of ICT than their child. The school will, therefore, take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and website information about national/local e-safety campaigns/literature. Parents/carers will be responsible for: ● Endorsing (by signature) the Pupil Acceptable Use Policy ● Accessing the school website in accordance with the school's Acceptable Use Policy
Community Users	Requests for access to the school's ICT systems by community users will be considered on an individual basis and must be approved by the Headteacher. Community users will be responsible for: ● Using the school's ICT systems in accordance with the appropriate Community Users Acceptable Use Policy, which they will be expected to sign before being given access to school systems

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils 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.
- Pupils are not allowed to freely search the internet.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT/ Designated Lead(s) for Safeguarding (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear

reasons for the need and be approved in advance by a member of the Senior Leadership Team.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education and Training – Staff

It is essential that staff, according to their role, receive e-safety training and understand their responsibilities as outlined in this policy. Briefings will be offered as follows:

- Formal e-safety briefings will be made available to staff. An audit of e-safety training needs of all staff will be carried out regularly and a log kept of all training undertaken. All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand and sign the school's Acceptable Use Agreement.
- The Designated Lead(s) for Safeguarding will receive regular updates through the LA / other information / training sessions and by reviewing guidance documents released by the SWGFL, the Local Authority, Multi Academy Trust and others.
- The Designated Lead(s) for Safeguarding will provide advice, guidance and training to individuals as required.
- E-Safety briefing and updates will be delivered to school staff as part of the first INSET day of each academic year. The E-Safety Policy will be discussed. Further training and updates will be provided as staff/team meetings as appropriate.

Training – Governors

The nominated E-safety and Safeguarding governors will take part in e-safety awareness sessions

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school briefing sessions for staff or parents
- Ad hoc meetings with the Designated Lead(s) for Safeguarding and/or the ICT technician

Education and Information for Families

Many 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 online experiences. Parents often either underestimate or do not realise how often children and young people come across

potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

Everyone has a role to play in empowering children to stay safe while they enjoy these technologies, just as it is everyone’s responsibility to keep children safe in the non-digital world. The school will, therefore, seek to provide information and awareness to parents and carers through:

- Letters, newsletters and school web site
- Parents’ evenings
- ICT agreements

Technical – Infrastructure/Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the IDN Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All staff users will be provided with a username and password by the ICT technician. Children will all provided with a username and a class log-in password in key stage one and a personal username and password in years 3-6. The ICT technician will keep an up to date record of users and their usernames. Users will be required to change their password annually.
- The “master / administrator” passwords for the school ICT system, used by the ICT Technician, among others, must also be available to the Headteacher or other nominated senior leader and kept in a secure place (school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by IDN
- In the event of the ICT technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or member of SLT
- Any filtering issues should be reported immediately to IDN
- Requests from staff for sites to be removed from the filtered list will be considered by the Designated Teacher(s) for Safeguarding, if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Governor

- School ICT/E-safety staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident to the Designated Teacher(s) for Safeguarding
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, laptops and handheld devices from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access of "guests" i.e. supply, trainee teachers, visitors onto the school system, via separate supply teacher log-ins
- Staff are informed at induction that they are forbidden to install programs on school workstations/network/portable devices; programs can be requested through the ICT/Designated Teacher(s) for Safeguarding
- An agreed procedure for staff is in place stating the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Procedures for taking Documents/Equipment/Media Offsite

From time to time it may be necessary to take school documents, equipment or media off site, either for the purpose of working at home or at another location (e.g. networking with other educational establishments). In such circumstances, staff have a duty to ensure, as far as is possible, the safety and security of the item(s) taken off site. The loss of information or equipment, whether containing confidential or sensitive material or not, may affect the rigour of our safeguarding measures, compromise data protection and can seriously damage the reputational standing of the school. Therefore, this may result in disciplinary proceedings being instigated.

The following protocol should be followed:

- Documents/equipment/media will not be taken off site without the knowledge and/or permission of the Headteacher.
- Confidential/sensitive items will not be taken offsite without the specific permission of the Headteacher.
- All items remain the responsibility of the member of staff who has taken them off site.
- All items will be clearly identifiable as being the property of the school (i.e. labelled with the school name and postcode), confidential/sensitive material will also be clearly labelled and memory sticks encrypted, laptops encrypted/password protected

- During transportation all items will be secured, out of site, in the locked boot of the car. Items will not be left unattended in a car and staff will check their car insurance to ensure that such items are covered for damage or theft
- Items will not be left unattended at home or offsite where they may be susceptible to unauthorised access. The use of school owned equipment / media by family or friends is strictly prohibited
- Staff will not store confidential/sensitive items on laptops (unless encrypted and, where necessary, saved on a memory stick)
- Staff will not retain items off site unnecessarily, returning all items to the school as soon as the work is finished
- Staff will report any misuse, loss or damage to the Headteacher immediately.

Use of Digital and Video Images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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
- Staff are allowed to take digital/video images to support educational 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
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on 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, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers

Data Protection

Staff should be aware that data on pupils and their families is covered by Data Protection legislation. This policy is written to include the principles that staff must follow to be compliant.

School Password Security

A safe and secure username/password system is essential if the school is to ensure that the school infrastructure/network is as safe and secure as possible. This will apply to all school ICT systems, including email and Virtual Learning Environment (VLE), so that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- Access to personal data is securely controlled in line with data protection. school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT technician and will be reviewed, at least annually, by the E-Safety Governor.

All staff and pupils at KS2 will be provided with a username and password by the ICT/Designated Lead(s) for Safeguarding who will keep an up to date record of users and their usernames.

In the interests of everyone's professional and personal safety, the following protocol will be followed by staff and pupils:

- The account will be "locked out" following six successive incorrect logon attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, will be change immediately after the first log-on.
- Passwords shall not be displayed on screen and shall be securely hashed.
- Requests for password changes should be authenticated by Designated Teacher(s) for Safeguarding or Headteacher to ensure that the new password can only be passed to the genuine user
- Never reveal passwords to anyone
- Never use the 'remember password' function
- Do not use the same password for systems inside and outside of work
- Do not use any part of username within the password
- Never write passwords down or store them where they are open to theft.
- Never store passwords in a computer system without encryption

- Use ‘strong’ passwords (use of symbols and characters)
- Change your password at least every two terms
- Passwords for the school website should also be changed 3 times per year

The “master / administrator” passwords for the school ICT system, used by the ICT Technician, must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. The school will never allow one user to have sole administrator access.

Responsibilities

The management of password security will be the responsibility of the Designated Lead(s) for Safeguarding.

All adults and pupils (except EYFS & KS1 who will use a ‘class log-on’) will have responsibility for the security of their username and password, must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users can be allocated by the ICT/Designated Lead(s) for Safeguarding. Any changes carried out must be notified to the Designated Lead(s) for Safeguarding.

Training

Members of staff will be made aware of the school’s password procedures:

- At induction
- Through the school’s e-safety policy.
- Through the Acceptable Use Agreement

Pupils will be made aware of the school’s password procedures:

- In ICT and / or e-safety lessons
- Through the Acceptable Use Agreement

Monitoring and Review of Password Security

The ICT Technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority or Multi Academy Trust auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. The password security section

of this policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.

In the event of discovering or suspecting inappropriate use of the web, the procedures outlined in the Acceptable Use Policy Agreement will be followed.

What to do if you Discover or Suspect Illegal Activity on the Web.

Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the Headteacher and the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the Designated Lead(s) for Safeguarding or Headteacher attempt to conduct an investigation of their own or bring in an outside 'expert' to do so as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

IT IS VITAL THAT EVIDENCE IS PRESERVED

Responding to Incidents of Misuse

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

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The SWGfL flow chart should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the 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 as defined in the Multi Academy Trust and School.

Communications

A wide range of rapidly developing communication technologies has potential to enhance learning. However, these must be used in accordance with the information below.

- The official school email service may be regarded as safe and secure and 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 need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Mobile Phones usage by Pupils

The school recognises that some parents will wish their child to carry a mobile phone so that they may communicate with them before and after the school day. This is restricted to year 6 pupils only.

The following protocol will be followed:

- Mobile phones will be switched off during the school day and not be switched on until the pupil has left the school premises at the end of the day.
- Pupils will hand their mobile phones into the school office at the beginning of the day where it will remain until the end of the day.
- Pupils will not take mobile phones on school trips or to offsite activities such as sports events. If the pupil is not returning to school after the event, the phone will be left in the care of the teacher in charge until they are collected.

Any breach of these rules may result in sanctions being applied in accordance with the school's behaviour policy

Mobile Phones usage by Staff

It is accepted that the majority of members of staff will have their mobile phone with them at work. To comply with the E-Safety Policy the following protocol will be followed:

- Members of staff will act as role models in their use of mobile phones.
- Personal mobile phones remain the responsibility of the member of staff at all times.
- Mobile phones will be switched off or on silent mode during the school day.
- Mobile phones will not be used whilst involved in the teaching or supervision of children, use of the phone will be limited until break time/non-contact time during the school day.
- Personal mobile phones **MUST NOT** be used to store personal information relating to pupils or parents/ carers.
- Mobile phones **MUST NOT** be used to take or store photographs/video of pupils or parents.
- Personal mobile phones must not be used as a means of communication with pupils or parents/carers, unless not to do so places the child at risk of harm.
- The use of personal mobile phones to access inappropriate material/websites whilst on site/during contractual hours is strictly prohibited.

JUly 2016

Review July 2017