E-Safety Policy
January 2019

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 new 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 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. This school e-safety policy is designed to help ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Radicalisation to support terrorism
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual’s consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

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 other school policies (e.g. behaviour, anti-bullying 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 students’ 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.

Scope of the Policy

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 school ICT systems, both in and out of school.

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 e-safety behaviour that take place out of school.
Roles and Responsibilities
The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:
Governors are responsible for:
• the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher:
• is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Subject leader who is also the E-Safety Co-ordinator.
• must ensure they undertake regular training and make sure and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
• and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Subject Leader / E-Safety Coordinator
• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• provides training and advice for staff
• liaises with the Local Authority
• liaises with school ICT technical staff
• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
• meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
• attends relevant meeting / committee of Governors

Technical staff:
The ICT Technician is responsible for ensuring that:
• monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff
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, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
• digital communications with pupils (email / Learning Platform - DB Primary) should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other school activities
• pupils understand and follow the school e-safety and acceptable use policy
• 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 hand held 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

**Designated person for child protection / Child Protection Officer:**
should be trained in e-safety issues and be aware of the potential for serious child protection 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

**Pupils:**
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school.

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (At KS1 parents can sign on behalf of the pupils).

**E-safety Officers:**
E-safety officers will be selected from Year 5 every two years, to enable them to continue and develop their role into Year 6. They are responsible for:
• sharing information with pupils about e-safety
• liaising with ICT co-ordinator and CPO to plan and deliver assemblies and activities.
• informing ICT co-ordinator of any e-safety issues brought to their awareness.

**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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:
• endorsing (by signature) the Student / Pupil Acceptable Use Policy
• accessing the school website/learning platform in accordance with the relevant school Acceptable Use Policy.

**Education / Training**

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

E-Safety education will be provided in the following ways:
A planned e-safety programme will be provided as part of the ICT curriculum, through the school's long-term planning adopted from DB Primary. E-safety will also be a focus in PSHE lessons and will be regularly revisited. (This will cover both the use of ICT and new technologies in school and outside school)

Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities, delivered by staff, e-safety officers and community police officers.

Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Rules for use of ICT systems / internet will be posted in the ICT suite and all classrooms

Staff should act as good role models in their use of ICT, the internet and mobile devices.

Parents / carers:
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 on-line 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).

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

- Letters, newsletters, web site, learning platform (DB Primary)
- Parents’ evenings
- Reference to the NSPCC e-safety page on the school’s website.

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The ICT Subject leader / E-Safety Coordinator will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The ICT Subject leader / E-Safety Co-ordinator will provide advice / guidance / training as required to individuals as required.
- All staff receive Prevent training, ensuring that children are safe from terrorist and extremist material when accessing the internet in school. As with other online risks of harm, every teacher is aware of the risks posed by the online activity of extremist and terrorist groups.
- All staff have all read Part 1 of the 'Keeping Children Safe in Education' guidance document.
Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:
• Attendance at training provided by the Local Authority or other relevant organisation.
• Participation in school training / information sessions for staff or parents.

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.

• School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the 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 users will have clearly defined access rights to school ICT systems.
• The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g, school safe)
• Users will be made responsible for the security of their DB Primary username and password, must not allow other users to access the systems using their log on 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 Halton LA.
• Any filtering issues should be reported immediately to the Headteacher and Halton LA.
• Requests from staff for sites to be removed from the filtered list will be sent to Halton LA.
• 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.

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.
• Where pupils are allowed to freely search the internet, e.g., using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (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.
• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
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. There are many reported incidents of employers carrying 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.
• 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 or blog, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of the AUP signed by parents or carers at the start of the year.)
• Pupil’s work can only be published with the permission of the student / pupil and parents or carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

• used fairly, lawfully and transparently
• used for specific, explicit purposes
• used in a way that is adequate, relevant and limited to only what is necessary
• accurate and, where necessary, kept up to date
• kept for no longer than is necessary
• handled in a way that ensures appropriate security, including protection against unlawful or authorised processing, access, loss, destruction or damage.

Staff must ensure that they:

• At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse.
• 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, USB stick or any other removable media:
• the data must be encrypted and password protected
• the device must be password protected (many memory sticks / cards and other mobile devices cannot 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 school policy (below) once it has been transferred or its 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 benefit of using these technologies for education outweighs their risks / disadvantages:
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. 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 e-mail communications may be monitored
• Users must immediately report, to the nominated person – in accordance with the school policy, 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, DB primary) 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 for these communications.
• Individual DB Primary e-mail addresses are used from Year 1 to Year 6, but can only be used within DB Primary.
• Any inappropriate language used in DB Primary e-mails will be flagged, and a message will be sent to the class teacher and administrator.
• All pupils are assigned a Google Mail e-mail address, which are given to them in upper KS2.

Pupils should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
• Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

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
• terrorism or extremism
• other criminal conduct, activity or material

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 follows:

<table>
<thead>
<tr>
<th>Incidents:</th>
<th>Refer to class teacher</th>
<th>Refer to DHT</th>
<th>Refer to Headteacher</th>
<th>Refer to Police</th>
<th>Refer to technical support staff for action</th>
<th>Inform parents / carers</th>
<th>Removal of network / internet access rights</th>
<th>Warning</th>
<th>Further sanction eg detention / exclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliberately accessing or trying to access material that could be considered illegal</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unauthorised use of non-educational sites during lessons</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unauthorised use of mobile phone / digital camera / other handheld device</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unauthorised use of social networking / instant messaging / personal email</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Allowing others to access school network by sharing username and passwords</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Attempting to access or accessing the school network, using another pupil’s account</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Attempting to access or accessing the school network, using the account of a member of staff</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Corrupting or destroying the data of other users</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Continued infringements of the above, following previous warnings or sanctions</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Actions which could bring the school into disrepute or breach the integrity of the ethos of the school</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Using proxy sites or other means to subvert the school’s filtering system</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Accidentally accessing offensive or pornographic material and failing to report the incident</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Deliberately accessing or trying to access offensive or pornographic material</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Approved: ..................................................................................................................................................

Date: ...........................................Review Date: .................................................................