BICKLEY PRIMARY SCHOOL

Digital Technologies & Internet Safety Policy

Agreed: November 2010

Reviewed: March 2017

Review date: March 2020

BICKLEY PRIMARY SCHOOL

Digital Technologies & Internet Safety Policy

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 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
- 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
- Sexting
- 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.
- Radicalisation

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 (eg Behaviour, Anti-bullying, Preventing Radicalisation and Safeguarding 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.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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 Computer systems (including laptop trolleys and ipads), both in and out of school.

The Education 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 safety incidents covered by this policy, which may take place out of school, but is linked to membership of the 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:

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including internet-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the ICT Leader
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Leader and other relevant staff receive suitable CPD to enable them to carry out their internet-safety roles and to train other colleagues, as relevant
- The Senior Leadership Team will receive regular monitoring reports from the Computing Leader.
- The Headteacher and another member of the Senior Leadership 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. (see “What do we do if...?” later in the document) This also refers to the staff Code of Conduct and Safeguarding Policy.

Computing Leader:

- takes day to day responsibility for internet-safety issues (along with the head teacher) and has a leading role in establishing and reviewing the school internet-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 IT technical staff

- receives reports of internet-safety incidents and creates a log of incidents to inform future internet-safety developments (kept with safe-guarding incidents in HTs Office)
- attends relevant meeting / committee of Governors when invited
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / IT Technician / Computing Leader is responsible for ensuring:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the internet-safety technical requirements outlined in the LGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Internet-Safety Policy and guidance
- that users may only access the school's networks with a protected password
- LGfL is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with internet-safety technical information in order to effectively carry out their safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (Fronter) / email is monitored in order
- that any misuse / attempted misuse can be reported to the relevant person

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of internet-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)
- they report any suspected misuse or problem to the Computing Leader / Headteacher for investigation / action / sanction
- digital communications with pupils (Fronter) should be on a professional level and only carried out using official school systems
- Internet-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school internet-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor Computing activity in lessons, extra-curricular and extended school activities
- they are aware of internet-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

• Reporting access of inappropriate websites to the headteacher for them to be blocked using the LGfL filtering system.

Designated Child Protection Officer

• should be trained in internet-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

• attempts to radicalise

Pupils:

• are responsible for using the school IT systems in accordance with the school rules and Acceptable Use Policy/Agreement (signed by them in KS2). (At KS1 the AUP will be looked at as a class and discussed with their teacher)

• have a good 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

• 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 internet-safety practice when using digital technologies out of school and realise that the school's Digital Technologies & Internet-Safety Policy covers their actions out of school, if related to their membership of the school

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. The school will take every opportunity to help parents understand this issue. Parents and carers will be responsible for:

• endorsing (by signature) the Acceptable Use Policy for parents/carers

• accessing the school website / Fronter / in accordance with the relevant school Acceptable Use Policy.

Policy Statements
Education – 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.

Digital Technologies & Safer Internet education will be provided in the following ways:

- A planned Internet-safety programme will be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of computing and new technologies in school and outside school
- 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 adopting safe and responsible use of Computing, 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
- Staff should act as good role models in their use of Computing, the internet and mobile devices

Education & Training – Staff

It is essential that all staff receive Digital Technologies & Internet-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 if they recognise it as a need.
- All new staff should receive information as part of their induction programme, staff handbook, ensuring that they fully understand the school Digital Technologies & Internet-safety policy
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days
- The Computing Leader will provide advice / guidance / training as required to individuals as necessary
- The Computing Leader, with the support of the Curriculum Development Team will provide advice / guidance / training as required to parents and carers as necessary

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 computer systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- Servers, wireless systems and cabling are secured when the building is vacant
- All users will be provided with a username and password by the IT Technician who will keep an up to date record of users and their usernames.

- Users will be made responsible for the security of their 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 LGfL
- Any filtering issues should be reported immediately to LGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Computing Leader.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

Digital Technologies & Internet-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of Computing 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Where pupils are members of sites such as “Scratch” where members of the public can upload pictures, programs and other forms of information
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked
- 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

Data Protection

Personal data will be recorded, processed, transferred and made available according 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 than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection.

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:

	STAFF				PUPILS			
	allowed	Allowed at certain times	Allowed for selected staff	Not allowed	allowed	Allowed at certain times	Allowed with staff	Not allowed
Pupils' mobile phones may be brought to school in exceptional circumstances but must be stored in the office	☑				☑			
Staff mobile phones may be brought to school but must be on silent and stored securely during lesson times	☑							
Use of mobile phones in lessons				☑				☑
Use of mobile phones in social time	☑							☑
** Taking photos on camera devices which are the property of the school, other than mobile phones; data to remain in school/on school devices	☑						☑	
Taking photos on camera devices and uploading them to a public or limited public website. Written permission must be sought.		☑				☑		
Taking photos on mobile phones				☑				☑
Use of hand held devices eg Ipads	☑				☑			
Use of personal email addresses in school, or on school network		☑						☑
Use of school email for personal emails				☑				☑
Use of forum in class area on Fronter	☑				☑			
Use of chat rooms / facilities				☑				☑
Use of instant messaging				☑				☑
Use of social networking sites				☑				☑
Use of blogs		☑					☑	

** The governors have agreed that parents may take photos of their children during the school's organised events (ie assemblies, public performances, sports).

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.
- Storage of secure files on Fronter (e.g. Governors Confidential Room, Staffroom) may be regarded as a safe and secure and is monitored
- Users need to be aware that email 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, VLE etc) must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

		acceptable	Acceptable at certain times	Accepted for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download,	child sexual abuse images					☑
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☑
	adult material that potentially breaches the Obscene Publications Act in the UK					☑
	criminally racist material in UK					☑
	pornography				☑	

upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	promotion of any kind of discrimination					☑
	promotion of racial or religious hatred					☑
	Promotion of radical behaviour					☑
	Threatening behaviour, including promotion of physical violence or mental harm				☑	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☑	
Using school systems to run a private business					☑	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the school					☑	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					☑	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					☑	
Creating or propagating computer viruses or other harmful files						☑
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					☑	
On-line gaming (educational)		☑				
On-line gaming (non educational)			☑			
On-line gambling					☑	
On-line shopping / commerce				☑		
File sharing					☑	
Use of social networking sites					☑	
Use of video broadcasting eg Youtube			☑			

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/Computing Leader and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools raise an issues through the management site – HT or Computing Leader).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC, laptop or tablet.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC, laptop or tablet to a secure place.
   - Instigate an audit of all IT equipment by the schools IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC, laptop or tablet to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including anti-bullying and PSHEC and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.

6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA .

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.

2. Secure and preserve any evidence.

3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.

4. Endeavour to trace the origin and inform police as appropriate.

5. Inform LA

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.

2. Advise the child on how to terminate the communication and save all evidence.

3. Contact CEOP http://www.ceop.gov.uk/

4. Consider the involvement police and social services.

5. Inform LA

6. In the case of radicalisation: Jill.Bartlett@met.pnn.police.uk

SO15 Counter Terrorism Intelligence Officer - Bromley & Lewisham

728776 / 728444 07769 164201

Robert.P.Affleck@met.police.uk

PC 1402CT Robert Affleck

Prevent Engagement Officer

M 07775 036482

7. Consider delivering a parent workshop for the school .community.

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

1. There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:
   - Whether there is an immediate risk to a young person or young people
     When assessing the risks the following should be considered:
     - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
     - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
     - Are there any adults involved in the sharing of imagery?
     - What is the impact on the pupils involved?
     - Do the pupils involved have additional vulnerabilities?
     - Does the young person understand consent?
     - Has the young person taken part in this kind of activity before?
   - If a referral should be made to the police and/or children's social care
   - If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
   - What further information is required to decide on the best response
   - Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown
   - Whether immediate action should be taken to delete or remove images from devices or online services
   - Any relevant facts about the young people involved which would influence risk assessment
   - If there is a need to contact another school, college, setting or individual
   - Whether to contact parents or carers of the pupils involved - in most cases parents should be involved
2. An immediate referral to police and/or children's social care should be made if at this initial stage:
   - The incident involves an adult
   - There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
   - What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
   - The imagery involves sexual acts and any pupil in the imagery is under 13

- You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

3. If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).
4. The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

All of the above incidences must be reported immediately to the head teacher.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

School Filtering Policy

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the London Grid for Learning (LGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Headteacher/Network Manager / ICT Technician / Computing Curriculum Leader. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. All users have a responsibility to report immediately to the relevant person any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Computing education programme.

They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:

- Staff code of Conduct
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Parent Handbook and through the monthly newsletter or Curriculum Evening (where appropriate) etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Computing Leader or Network Manager who will decide with the headteacher whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at LGfL level, then the responsible person should use the secure access through the LGFL Portal (Headteacher or Computing Leader only) to contact the helpdesk.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will monitor the activities of users on the school network and on school equipment as indicated in the School Digital Technologies & Internet SAfety Policy and the Acceptable Use agreement.

Signed …………………………………………. ……………………………………………….
Chair of Governors

Dated:

Reviewed March 2017

Date on which policy was first approved: 25 November 2010