eSafety policy

eSafety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images. The school has a designated eSafety coordinator. This policy applies to all members of the Brookwood Primary School community (including staff, pupils, volunteers, parents, visitors and community users) who have access to and are users of school ICT systems.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the eSafety Governor. The role of the eSafety Governor includes:

- regular meetings with the eSafety Co-ordinator
- regular monitoring of eSafety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors

Headteacher:

- Has a duty of care for ensuring the safety (including eSafety) of members of the school community.
- Is aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff
- Is responsible for ensuring that the eSafety Coordinator and other staff receive suitable training to enable them to carry out their eSafety roles
- Is responsible for ensuring that internal eSafety monitoring takes place
- Liaises with the Bourne Education Trust on matters of eSafety
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments

eSafety Coordinator :

- Has day to day responsibility for eSafety issues and establishes and reviews the school eSafety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Provides training and advice for staff

Network Manager (Bourne Education Trust):

The Network Manager ensure that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required eSafety technical requirements and all BET policies or guidelines that apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Use of the network is regularly monitored in order that any misuse / attempted misuse is reported to the Headteacher for investigation
- Monitoring software is implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of eSafety matters and of the school eSafety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- All digital communications with pupils, parents or carers is on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the eSafety Policy and acceptable use policies
- Pupils have a good understanding of research skills
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Ensuring that, in lessons where internet use is pre-planned, pupils are 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

Training is offered to staff as follows:

- eSafety training is regularly updated and reinforced. An audit of the eSafety training needs of all staff is carried out as part of Performance Management.
- New staff receive eSafety training as part of their induction programme, ensuring that they fully understand the school's eSafety Policy and Acceptable Use Agreements.

Designated Safeguarding Lead

The DSL is trained in eSafety issues and is aware of the potential for serious child protection / 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

Pupils:

- Are responsible for using the school's digital technology systems in accordance with the rules established by their teacher
- Have a good age-appropriate understanding of research skills
- Know how to report abuse, misuse or access to inappropriate materials
- Know the importance of adopting good eSafety practice when using digital technologies out of school and realise that the School's eSafety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The School takes opportunities to help parents understand these issues through parents' evenings, newsletters and the school website. Parents and carers will be encouraged to support the school in promoting good eSafety 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 (when allowed)

Community Users

Community Users who access school systems as part of the wider school academy provision are expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality ICT experiences as part of their learning.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by ***** and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Pupils are educated in safe searching when using the Internet, and will be directed to safe and age-appropriate digital resources.
- Pupils are shown how to publish and present information appropriately to a wider audience.
- Pupils are taught how to use online communication tools effectively and safely.

Pupils are taught how to evaluate Internet content

- The school seeks to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books.
- Pupils are taught how to report content that concerns them to a member of teaching staff.

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly.
- Virus protection is updated regularly.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and is monitored.
- Incoming e-mail where the author is unknown will be treated as suspicious and attachments not opened.

Published content and the school web site

- The contact details on the website is restricted to the school's address, e-mail and telephone number. Staff and pupils personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers is obtained before photographs of pupils are published on the school website.
- Pupils' full names are not used on the school web site, particularly in association with photographs.

S**ocial networking and personal publishing**

- The use of social networking sites in school is not allowed.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils through parent eSafety meetings, through newsletters and Parent Mail.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

- The school works in partnership with the Bourne Education Trust to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the eSafety Coordinator.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras are not used during lessons or formal school time.
- Staff will use a school phone where contact with pupils or parents is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to General Data Protection Requirements

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- Teaching staff demonstrate effective use of the internet and access to the Internet is by direct adult supervision using approved on-line materials.
- Any person not directly employed by the school are asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BET Academy can accept liability for the material accessed, or any consequences of Internet access. The school audits ICT use and emergence of new technologies to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate and effective.

Handling eSafety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- 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 consequences for pupils misusing the Internet. Community use of the Internet.
- All use of the school Internet connection by community and other organisations shall be in accordance with the school eSafety policy.

Technical considerations

The school is responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- The safety and security of the school's technical systems are audited regularly
- Equipment is securely located and physical access is restricted
- Users have clearly defined access rights to school devices

- From KS2 and upwards, including adults, users are provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password regularly
- The "master / administrator" passwords for the school, used by the Network Manager (or other person) also available to the Headteacher and kept in a secure place
- The Bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- **Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet**
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The school is moving towards eliminating the use of removable media, including memory sticks. In the meantime, encrypted devices are made available. Personal data is not sent over the internet or taken off the school site unless safely encrypted.
- Use of the school's internet password is restricted to ******

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. There are, however, risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website / social media / local
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers 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 is not 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 are not used anywhere on a website or blog, particularly in association with photographs
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data is recorded, processed, transferred and made available according to General Data Protection Regulations. In support of this, staff must:

- 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, memory stick or any other removable media:

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

Communications

- The school email service may be regarded as safe and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate school business. The email system is not secure, and Egress or password-protected files must be used when transferring any personal data.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used for pupils throughout school
- Pupils are taught about eSafety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the school academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Brookwood School does not currently use social media. Staff who use social media outside school are required to comply with the Code of Conduct and Acceptable Use Policy.

Staff ensure that:

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school may effectively respond to social media comments made by others Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying is also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	

	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing					X	
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube			X			

Approved at CPW Committee: June 2019
Date for next review: June 2020