Online Safety, ICT & Digital Devices

Acceptable Use Policy

January 2024

BARHAM

PRIMARY SCHOOL

Reviewed by:	**Designated Safeguarding Lead & Online Safety Officer**
Approved by:	**Filtering & Monitoring Governor**
Last review date:	**January 2024**
Date Approved:	**February 2024**
Review Process:	**Biyearly**
Review Date	**February 2025**

Contents

Introduction and aims of the policy

This document aims to safeguard pupils and staff from ICT related issues and ensure that the HPS community is safe online. It ensures that digital devices and resources are used safely and in a professional manner.

Online Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of online safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about student welfare and safety as well as how to protect pupils and staff from risks and infringements.

All staff have a responsibility to support online safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach online safety protocols. Online safety is a concern that is not limited to school premises, school equipment or the school day. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyberbullying will be dealt with in accordance with the school's behaviour policy. Online safety issues relating to safeguarding will be dealt with in accordance with the school's safeguarding policy.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Why ICT systems, devices and the Internet are important to our pupils and staff

The purpose of ICT and Internet use in school is to raise standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Benefits of Internet use for education:

- The Internet is a part of the statutory curriculum and a necessary tool for staff and pupils and it benefits education by allowing access to worldwide educational resources as well as enabling access to specialists in many fields for pupils and staff;

- Access to the Internet supports educational and cultural exchanges between students worldwide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home;
- The Internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data;
- The Internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives;
- The Internet offers opportunities for mentoring pupils and providing peer support for them and their teachers;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Pupils will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Management of information on the school website

Editorial guidelines will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised.

The point of contact on the web site will be the school address, school email and telephone number. Staff or pupils' home information will not be published.

Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Parental permission will be obtained for taking photographs of pupils and publishing them on the school web site or any publications. Photographs will be published in accordance with GDPR guidelines. A senior member of staff will oversee / authorise the website's content and check suitability. Uploading of information will be restricted to certain staff members. Digital images/video of pupils will be stored in a secured area of the network. Website compliance will be audited on a yearly basis or to reflect changes in statutory guidance.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Managing information held by the school

The school conducts regular information audits to gain a clear and common understanding of the range of information assets it holds and those that are critical to business and ensure GDPR compliance. Personal data sent over the network or to appropriate external agencies will be encrypted or otherwise secured.

Use of digital and video images

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 recognize the risks attached to publishing their own images on the Internet.

Staff are allowed to take digital/video images, using school equipment, to support educational aims, but follow school policies concerning the sharing, distribution and publication of those images.

Care should be taken with 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.
HPS will not use images of pupils publicly or externally whose parents or carers have not explicitly given their permission to do so.

Staff must report any concerns relating to any inappropriate or intrusive photography to the Designated Safeguarding Lead or Head Teacher.

Staff must not use any images that are likely to cause distress, upset or embarrassment.

Photographs taken by staff on school visits may be used in the curriculum and displayed within school or at parents' evenings to illustrate the work of the school except in cases where the parent/carer has opted their child out.

Social networking and chat rooms

Pupils will not be allowed to access public or unregulated chat rooms or forums. Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

Newsgroups will be blocked unless an educational need can be demonstrated.

Staff will not exchange social networking addresses or use social networking sites to communicate with parents, unless permission has been granted by the Head Teacher.

Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil/parent is necessary, the agreement of a senior manager should always be sought first, and language should always be appropriate and professional.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Barham Primary School recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming and/or expose pupils to harmful content). For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real.

Barham Primary School will treat any use of AI to access harmful content or bully pupils in line with this policy and our behaviour and anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Managing email

All staff and pupils must have signed the 'Acceptable Use of Digital Devices' policy before being allowed access to the school's email service.

The school's email system includes a filter to help prevent spam and other unwanted emails.

Personal email or messaging between staff and pupils should not take place.

Staff must use their school email address if they need to communicate with pupils about their school work.

Pupils and staff may only use approved email accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive email.

Pupils must not reveal details of themselves or others in any email communication such as an address or telephone number and must not arrange meetings with anyone.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and may be restricted.

The forwarding of 'chain letter' emails is not permitted.

Incoming emails should be regularly monitored, and attachments should not be opened unless the author is known to minimise the threat of viruses and phishing attacks.

Best practice guidelines for using email are included as an appendix to this policy.

Managing mobile phones and digital devices

Mobile phones should not be used by staff on the school premises (excluding break times).

The sending of abusive or inappropriate text messages, sounds, images, videos or other files is forbidden and will be dealt with in accordance with the school's Code of Conduct Policy.

Pupils are not permitted to use the cameras in their mobile phones or digital devices without the express permission of a member of staff. Use of the camera in a pupil's own device should be in accordance with the information set out in this policy.

Staff may be issued a digital device by the school, such as a tablet or laptop computer, to support Teaching and Learning and/or duties associated with a staff member's job description.

Digital devices issued by the school to staff or pupils must be used in accordance with the school's 'Acceptable Use of Digital Devices' policy both within the school and outside.

School-owned digital devices should pass through the school’s Internet filter to monitor use and help prevent staff or pupils accessing inappropriate material. Devices will be centrally managed and security settings will be applied to them to protect the devices. Where possible, GPS tracking will be deployed in case of theft or loss.

Images or videos that are taken of activities involving pupils must be captured using a school-owned device and not a personal device.

Authorising Internet access

All staff and pupils must read and sign the ‘Acceptable Use of Digital Devices’ policy before being allowed controlled access to the Internet.

The school will maintain a current record of all staff and pupils who are allowed access to the school’s ICT systems.

Parents/carers will be asked to sign and return the school’s form stating that they have read and understood the school’s ‘Acceptable Use of Digital Devices’ policy and give permission for their child to access ICT resources.

Staff will supervise access to the Internet for all students.

Filtering and monitoring systems

The school will work in partnership with parents/carers, the DfE, partners and the Internet Service Provider to ensure appropriate filtering and systems are implemented to protect pupils and staff and that these are reviewed and improved regularly.

These systems will ensure that there are effective anti-malware defences in place across all business functions that have in-built automatic scanning facilities at regular intervals of the day such that any changes can be made as a result of monitoring results.

If staff or pupils discover unsuitable sites, the URL and content must be reported to the Network Manager or a Designated Safeguarding Lead/Online Safety Officer.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF (Internet Watch Foundation) and CEOP (Child Exploitation & Online Protection Centre).

Regular checks by Network Manager and Designated Safeguarding Lead/Online Safety Officer will ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering methods will be age and curriculum appropriate.

Filtering will provide a safe environment for pupils to learn in whilst also avoiding ‘over blocking’.

User education and awareness

It is essential that staff and other adults working at the school are confident about using the Internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies. All staff are governed by the terms of this policy and will be provided with a copy and its importance explained. All new staff will be given access to a copy of the policy during their induction.

Staff development in safe and responsible use of the Internet and email will be provided as required. Staff will be aware that Internet use will be monitored and traced to the original user. Discretion and professional conduct is essential. Senior managers will supervise members of staff who operate the monitoring procedures.

Backups and anti-virus software

All content that is saved to a shared or personal drive located on a server is backed up regularly.

All computers in the school have an anti-virus program with real-time scanning installed to prevent any damage or data loss caused by malicious files or programs.

The school's Network Manager and Technical Support Team are responsible for the installation and regular updating of the school's anti- virus and anti-malware software.

Removable storage controls

USB storage devices, portable hard drives, flash storage on mobile phones, SD cards from cameras, etc. carry a risk of infection so should not be used in school at any time. Personal and shared cloud storage is provided for all staff and pupils and should be used instead of removable storage devices.

Exceptions will be made to allow school-owned storage devices, such as the SD cards within school-owned digital cameras, to transfer files to computers in school.

ICT systems configuration and security

The school keeps a record of all ICT assets owned by the school. Assets are marked with a unique identifying number.

All devices require a password/passcode to use them. Computers are built from a pre-defined, school maintained, central image with security features pre-installed. Security patches are automatically downloaded and installed at their earliest opportunity.

Applications are deployed automatically to appropriate computers according to the terms of their licenses.

Password security is enforced for all staff, and staff should only change their password if there is a security breach.

The school has effective account management processes and users will be given appropriate and controlled access to the network. Accounts are automatically created and deactivated based on the staff member's or pupil's status in the school's management information system.

Administrative access to the network is limited, and the accounts which have this privilege are monitored and assessed by the Network Manager.

If an individual needs to access an area of the network to which they do not currently have access, a request should be made to the Network Manager.

All CCTV footage from the school's cameras is stored on a dedicated server. CCTV footage may also be made available on school computers that are located in secure, non-pupil areas (such as those offices used by Head Teacher and senior managers).

Reporting misuse of ICT facilities and the Internet

Responsibility for handling pupils' incidents will be delegated to a senior member of staff and the safeguarding team

Introducing this policy to staff and pupils

Pupils will be required to accept the 'Acceptable Use of Digital Devices' policy at the start of the academic year. These guidelines will also be posted in the ICT Suite.

All staff including teachers, supply staff, classroom assistants and support staff, will be required to accept the terms of the 'Acceptable Use of Digital Devices' policy before using any ICT resource. Staff will be made aware that Internet traffic could be monitored and traced to the individual user and that discretion and professional conduct is essential.

Parents and Carers as partners

Parents' attention will be drawn to this Policy in the newsletters and on the school website. Parents will be required to read the 'Acceptable Use of Digital Devices' policy with their child and sign the agreement. A partnership approach with parents will be encouraged. Information on cyber-bullying and safe use of the internet will be published on the school's website.

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parents/Carers factsheets - Childnet International
- Healthy relationships – Disrespect Nobody

Sanctions for the misuse of ICT systems and digital devices

Sanctions for the misuse of the Internet, ICT systems and school-owned digital devices used on the school premises include internal or external exclusions in accordance with the behaviour policy and dependent on the nature of the incident.

For more serious offences temporary removal of Internet access or computer access may be required, which could ultimately prevent access to files held on the system.

There may be occasions when the police will need to be contacted.

Appendices

Appendix A – Acceptable use of ICT and Digital devices – Pupil Agreement
Appendix B – Acceptable use of ICT and Digital devices – Staff Agreement
Appendix C – Staff Guidelines for Usage of School Emails
Appendix D – Mobile Digital Devices Acceptable Use Policy
Appendix E – CCTV Recording System Policy

Appendix A: Acceptable use of ICT and Digital devices – Pupil agreement

Barham Primary School provides pupils with access to its computer network and its Internet connectivity. Pupils are expected to behave responsibly on the school computer network. The school has a duty of care to its pupils and despite the immense educational potential of ICT and other digital services; there is an unpleasant side to the Internet and other technological devices including mobile phones. Pupils and their Parents/Carers are asked to read the following guidelines carefully, sign the Declarations and return the signed document to the school.

The term 'digital devices' extends to all information and communication technology devices including school ICT equipment, tablets, portable computers, removable storage devices or any device capable of connecting to the Internet.

1. The school uses monitoring software that detects any inappropriate use of the school's digital facilities to be traced to the individual concerned. The software monitors websites visited, any incidences related to cyber-bullying, pupils viewing pornographic images, racist abuse and the PREVENT and CSE strategies. The school has a web filtering service which is regularly updated. Pupils may make use of the school network, Internet connectivity and digital devices to enrich their studies.
2. Pupils must not use the camera/video facilities on digital devices to photograph/video other members of the school community without their consent. They must, under no circumstances, post or share image/video files of other members of the school community. Recordings of images deemed to be inappropriate using the school's digital facilities, including any showing violence or personal humiliation, are unacceptable and will be regarded as a serious offence.
3. Pupils must not access, upload, download, display, or distribute obscene, racist, sexist, abusive, unethical, unlawful or sexually explicit material on the school network that could bring the school into disrepute. If, by accident, pupils encounter any such sites, they should report it immediately to a member of staff who will arrange for it to be added to the school's web filter. Under no circumstances are pupils allowed to access any proxy anonymisers or VPNs.
4. Pupils are responsible for email messages they send and for contacts made. Email / images / messages should be written carefully and politely. Pupils will be given their own email address which should be used for all school-related communication. The use of forceful language or swearing is unacceptable. Pupils should exercise caution when opening email attachments, particularly if they are not expecting the email, or they do not recognise the sender.
5. If you decide to include material obtained from the Internet in your school work you should recognise that people who have contributed that material have 'ownership' of it (known as copyright), and to use it without acknowledging its source is a form of theft and it will not be accepted in work you claim as your own.
6. Computer systems are vulnerable to cyber-attacks and security systems are built into the network to prevent such attacks. Pupils should value the protection these give and never attempt to bypass or alter the security settings. Files should be transferred between home and school by using email or our named online cloud-based storage platforms.
7. Pupils must respect the school's digital devices and report any damage to a member of staff. The school will charge for any deliberate or reckless damage caused by pupils.
8. Access to the school's computer system must be through a pupil's authorised account only. Pupils must not give out or share their password. Their account will be automatically created when they join the school and disabled when they leave.
9. If pupils misuse the school facilities action will be taken by the school in accordance with the Behaviour Policy which may include temporary or permanent exclusion. For serious violations, the school may need to involve Social Services or the Police.

DECLARATION BY THE PUPIL AND PARENT/CARER TO BE SIGNED AND RETURNED TO THE SCHOOL

Declaration by the Pupil:

I have read and understood the Acceptable use of Digital Devices at Barham Primary School. I understand that I am responsible for the security of my account and for keeping my password secret. I understand that these rules apply where relevant to privately owned devices and to my behaviour in communicating with others, even when I am at home. I will use digital devices and the Internet in a responsible way and obey the rules at all times.

Signed: ______________ Full Name: (block capitals) __________________

Date: ___________________

Declaration by Parent/Carer:

I have read and understood the Acceptable use of Digital Devices at Barham Primary School. As the parent/carer of the pupil signing above, I will support him/her in following the Guidelines. I recognise that in spite of the school's filtering systems, some unacceptable material may be accessible on the Internet and I accept responsibility for encouraging my son/daughter to set appropriate standards to follow when using digital devices. I understand that pupils will be held accountable for their own actions.

Signed: ___________________ Full Name: (block capitals) __________________

Date: ___________________

All personal data collected about pupils and parents/carers is collected, stored and processed in accordance with the General Data Protection Regulation.

Appendix B: Acceptable use of ICT and Digital devices – Staff agreement

Barham Primary School provides staff with access to its computer network and its Internet connectivity. Staff are expected to behave responsibly on the school computer network. The school's ICT facilities are made available to staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on its computer network, computers, tablets or laptops or to monitor the use of these ICT facilities.

The term 'digital devices' extends to all information and communication technology devices including school ICT equipment, tablets, portable computers, removable storage devices or any device capable of connecting to the Internet.

1. The school uses monitoring software that detects any inappropriate use of the school's digital facilities to be traced to the individual concerned. The software monitors websites visited, any incidences related to cyber-bullying, viewing pornographic images, racist abuse and the PREVENT and CSE strategies. The school has a web filtering service which is regularly updated. Staff may make use of the school network, Internet connectivity and digital devices to enrich their professional activities.
2. Staff must not access, upload, download, display, or distribute obscene, racist, sexist, abusive, unethical, unlawful or sexually explicit material on the school network that could bring the school into disrepute. If, by accident, staff encounter any such sites, they should report it immediately to the Network Manager or a senior member of staff who will arrange for it to be added to the school's web filter. Under no circumstances are staff allowed to access any proxy anonymisers or VPNs.
3. Staff are responsible for email messages they send and for contacts made. Email/images/messages should be written carefully and politely. Staff will be given their own email address which should be used for all school-related communication. The use of forceful language or swearing is unacceptable. Staff should exercise caution when opening email attachments, particularly if they are not expecting the email, or they do not recognise the sender.
4. Computer systems are vulnerable to cyber-attacks and security systems are built into the network to prevent such attacks. Staff should value the protection these give and never attempt to bypass or alter the security settings. Removable devices should not be used in school and files should be transferred between home and school by using email or our named online cloud-based storage platforms.
5. Staff must respect the school's digital devices and report any damage to the Network Manager or Senior Manager.
6. Access to the school's computer system must be through a staff member's authorised account only. Staff must not give out or share their password. Their account will be automatically created when they join the school and disabled when they leave.
7. Staff should change their password at least every 120 days. Passwords must conform to the school's complexity requirements.
8. Staff with responsibility for managing and accessing personal data in the school's management information system or the school's learning platforms will comply with the following conditions:
    a. The data is to be used only for educational purposes.
    b. Personal data is to be shared only with those who need the information to discharge a statutory education function.
    c. Only authorised users may access the system and they must never share their login details with anyone.
    d. Management of the school's learning platforms usernames and passwords is the responsibility of the Network Manager or Senior Managers in the school.

e. Care will be taken to protect any data which is printed or otherwise displayed in accordance with GDPR guidelines.
f. Temporary data sets will be deleted as soon as possible.

ECLARATION BY THE EMPLOYEE TO BE SIGNED AND RETURNED TO THE SCHOOL

I have read and understood the Acceptable use of Digital Devices at Barham Primary School.

Signed: __________________ Full Name: (block capitals) _________________________________

Date __________________________________

All personal data collected about pupils and parents/carers is collected, stored and processed in accordance with the General Data Protection Regulation. Please see our Privacy notices for further details.

Appendix C Staff Guidelines for Usage of School Emails

BPS Guidelines for the Usage of Emails

Email is a tremendously effective way of sharing information and managing work across the school. However, opening and responding to emails can be very time-consuming. We are conscious of the significant increase in workload as a result of dealing with email inbox and have reviewed the effective use of school communication system.

The following guidelines aim to reduce the number of emails in circulation consequently reducing the workload.

1. Think before you send an email. It might be easier to phone or meet in person. Keep email messages short and to the point. They are easier to read.

2. When replying, don't send a "reply to all" unless it is necessary for all the recipients to know your response. Think before you forward emails that you have received or a trail of previous emails. They may contain information that is confidential or expressly for you only.

3. Make the subject clear in the subject title of the email. Avoid multiple topics in the body of the message that do not match the title.

4. Do not treat an email like spoken communication. Email is a more informal medium than memos or letters, but it lacks the signals and clues that spoken language contains. For formal communication, please attach a letter to your email and send a hard copy to the concerned staff.

5. Avoid using UPPER CASE or oversized fonts, as the reader may feel that they are being shouted at (equivalent to raising your voice in a face to face conversation). Asterisks around a word are an *easy* way to add emphasis, if needed.

Staff should ensure that any electronic communication with students and staff are compatible with their professional role. Email messages must be about School business only. Staff should not give their personal contact details to pupils including personal e-mail. Staff should not use pupils’ personal e-mail addresses unless firmly within the boundaries of a professional context.

Appendix D - Mobile Digital Devices Acceptable Use Policy

The policies, procedures and information within this document apply to mobile digital devices, such as tablet or laptop computers or other Internet-connected devices and are in addition to the current ICT Acceptable Use Policy.

Users Responsibilities

1. Where relevant, users must use protective covers/cases for their device.
2. Care should be taken to prevent damage to the screens of mobile digital devices, particularly in devices where the screen is permanently exposed, such as a tablet computer.
3. Do not subject mobile digital devices to extreme heat or cold.
4. It is a user's responsibility to keep their device safe and secure. Do not store or leave unattended.
5. The whereabouts of your device should be known at all times.
6. School-owned digital devices are subject to routine monitoring. Users in breach of the Acceptable Use of Online Safety, ICT & Digital Devices Acceptable Use Policy may be subject to but not limited to: disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
7. Barham Primary School is not responsible for the financial or other loss of any personal files that may be deleted from a device.
8. Storage space on mobile digital devices can be quite limited. Academic content will take precedence over personal files and apps.
9. Users must use good judgment when using the camera. The camera should only be used in accordance with the guidelines set out in the ICT Policy.
10. Individual users are responsible for connecting a school-owned device to any home Internet connections and no support will be provided for this by the school.
11. Users should be aware of and abide by the guidelines set out by the school's ICT policy and Acceptable Use of Online Safety, ICT & Digital Devices Acceptable Use Policy.
12. The School reserves the right to confiscate and search any device to ensure compliance with the Acceptable Use of Online Safety, ICT & Digital Devices Acceptable Use Policy.
13. The device remains the property of Barham Primary School. The school retains the right to remove the device at any point in the future. If staff leave the employment of the school/pupils leave the school then the device should be returned to the school.
14. Care should be taken to log off any school systems when you have finished using them, and wherever possible you should not save the login details for any remote access connections.

Lost, damaged or stolen mobile digital devices

1. If a device is stolen, you will need to notify the police and obtain a crime reference number. It may be possible to claim a stolen device on the school's insurance, but only if the theft has been reported.
2. If you lose your device the Network Manager must be notified immediately. Loss is not covered by insurance. A replacement may be provided depending on the circumstances.
3. Where possible, devices that are believed to be stolen or lost will be tracked through GPS.

Name: ____

Signature: ____

Date: ____

Appendix E - CCTV Recording System Policy

1. Introduction

1.1. The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Barham Primary School hereafter referred to as 'the school'.

1.2. All CCTV footage is stored in the school's Server Room. CCTV may also be made available on school workstations that are located in secure, non-student areas (such as those offices used by Head Teacher and senior managers).

1.3. This document and information within complies with GDPR guidelines.

1.4. The CCTV system is owned by the school.

2. Objectives of the CCTV system

2.1 The objectives of the CCTV system are:

a To protect the school buildings and their assets
b To increase personal safety and reduce the fear of crime
c To support the Police in a bid to deter and detect crime
d To assist in identifying, apprehending and prosecuting offenders
e To protect members of the public and private property
f To assist in managing the school

3. Statement of intent

3.1. The operation of the CCTV System will be subject to the requirements of the GDPR regulations.

3.2. Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity that has occurred, is currently occurring, anticipated, or suspected, and for the purpose of securing the safety and wellbeing of the school, and its visitors.

3.3. The school will ensure that static cameras are not focused on private homes, gardens and other areas of private property.

3.4. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained from the Head Teacher.

3.5. Materials or knowledge secured from the use of CCTV will not be used for any commercial purpose. Recordings will never be released to the media for purposes of entertainment.

3.6. The planning and design has endeavoured to ensure that the System will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.7. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes to areas covered by the school CCTV.

4. Operation of the system

4.1. The System will be administered and managed by the Head Teacher.

4.2. The day-to-day management will be the responsibility of both senior staff and the Network Manager.

4.3. The CCTV system will be operated 24 hours each day, every day of the year.

5. Control / Server Room

5.1. The Network Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

6. Monitoring procedures

6.1. Camera surveillance of the site will be maintained at all times.

6.2. All cameras record to the CCTV system continuously.

7. Video recording procedures

7.1. In order to maintain and preserve the integrity of the recordings, clips are stored and viewed securely over the school network.

7.2. Recordings may be viewed by the Police for the prevention and detection of crime, authorised officers of London Borough of Brent for supervisory purposes, authorised demonstration and training and senior members of school staff.

7.3. A record will be maintained of the release of recordings to the Police or other authorised applicants.

7.4. Requests by the Police must be viewed onsite initially with a member of SLT present.

7.5. Should a recording be required as evidence, a copy may be released to the Police. Recordings will only be released to the Police on the clear understanding that the recording remains the property of the school, and both the recording and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the recording or any part of the information contained thereon.

7.6. The Police may require the school to retain the stored recordings for possible use as evidence in the future. Such recordings will be properly indexed and securely stored until they are needed by the Police.

7.7. Applications received from outside bodies to view or release recordings will be referred to the Head Teacher.

7.8. CCTV recordings will be kept, normally, for a minimum of 28 days.

8. Breaches of the code (including breaches of security)

8.1. Any breach of the Code of Practice by school staff will be initially investigated by the Head Teacher, in order for him/her to take the appropriate disciplinary action.

8.2. Any serious breach of the Code of Practice will be immediately investigated.

9. Assessment of the system and code of practice

9.1. Performance monitoring, including random operating checks, may be carried out by the authorised school staff.

9.2. Any complaints about the school’s CCTV system should be addressed to the Head Teacher.

9.3. Access by the Data Subject - GDPR regulations provides individuals with a right to data held about themselves, including those obtained by CCTV.

9.4. Requests for data relating directly to individuals should be made to the Head Teacher.

Summary of Key Points

- The CCTV system is owned and operated by the school.
- The Server room will only be staffed when the school is open.
- Liaison meetings may be held with the Police and other bodies.
- Recordings may only be viewed by Authorised School staff, the Technical Services Team or the Police.
- Recordings will not be made available to the media for commercial or entertainment purposes.
- Recordings will expire or be deleted securely.
- Any breaches of this code will be investigated by the Headteacher.
- Breaches of the code and remedies will be reported to the Headteacher.