CHBP School Federation

Brunswick Park Primary and Nursery School
Osidge Lane,
Southgate,
London
N14 5DU

Tel: 020 8368 3468
Email: office@brunswickpark.barnetmail.net

Church Hill Primary School
Burlington Rise
East Barnet
Hertfordshire
EN4 8NN

Telephone: 020 8368 3431
Email: office@churchhill.barnetmail.net

'As a federation, and as individual schools, we are committed to the wellbeing of all our community and endeavour to ensure that every member is valued regardless of age, gender, class, disability, ethnic heritage, religion, special educational needs or sexual orientations. We believe it is the right of all members of our community to be included in all aspects of school life, have access to school information and participate in all activities - these are integral parts of each school's culture and ethos. Policies are formulated and implemented with these principles in mind.'

Online Safety Policy

November 2021

	Date
APPROVED BY COMMITTEE / GB	
RATIFIED BY GOVERNING BODY (GB)	
NEXT REVIEW DUE	

Contents

1. Introduction and Overview 3
2. Managing the IT infrastructure 5
3. Data security 8
4. Equipment and Digital Content 8
5. Education and Curriculum 9
6. Expected Conduct and Incident management 10
Appendix 1 -Brunswick Park School e-Safety Policy: Staff Acceptable Use Agreement (Digital technologies) 13
Appendix 2a 16
I will only use the Internet and email with an adult 16
Appendix 2b - KS2 Pupil Acceptable Use of Technology Agreement 17
Appendix 3 - CHBP Online Safety Agreement Form: Parents 18

1. Introduction and Overview

Rationale and Scope
Our overall aim is:

- to protect and educate pupils and staff in their use of technology
- to have the appropriate mechanisms to intervene and support any incident where appropriate.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- exposure to terrorist and extremist material when accessing the internet
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Roles and Responsibilities

Role	Key Responsibilities
Executive Headteacher & Computing Lead	• To take overall responsibility for online safety provision • To be responsible for ensuring that staff receive suitable training • To be aware of procedures to be followed in the event of a serious online incident. • To have regular contact with other online safety committees, e.g. the local authority, Local Safeguarding Children Board. • To communicate regularly with school technical staff. • To communicate regularly with the designated safeguarding governor. • To create and maintain online safety policies and procedures. • To ensure that all staff are aware of the procedures that need to be followed in the event of an incident online. • To ensure that an online safety incident log is kept up to date. • To ensure children are safe from terrorist and extremist material when accessing the internet at school.
Computing Lead	• To oversee the delivery of the computing curriculum
Network Manager/technician	• To report any online safety related issues that arise to the designated safeguarding lead. • To ensure that access to the school network is only through an authorised, restricted mechanism • To ensure that provision exists for misuse detection and malicious attack. • To take responsibility for the security of the school IT systems. • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
Governors	• To ensure that CHBP Federation follows all current online safety advice to keep the children and staff safe.
Teachers	• To embed online safety messages in learning activities across all areas of the curriculum. • To supervise and guide pupils carefully when engaged in learning activities involving technology. • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's online safety policies and guidance. • To read, understand and adhere to the school staff Acceptable Use Policy.

Role	Key Responsibilities
	• To report any suspected misuse or problems to the Designated Safeguarding Lead. • To develop and maintain an awareness of current online safety issues and guidance. • To model safe and responsible behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.

How policy will be communicated

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Reference to policy to be made during induction of new staff and as part of September INSET each new year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held on file.

2. Managing the IT infrastructure

Internet access, security (virus protection) and filtering

CHBP:

- Has educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status; Computing Lead, Executive Headteacher, Capita IT Support staff.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to either pupils or staff;
- Has blocked pupil access to music & video download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Ensures network remains healthy through use of Sophos anti-virus software

Network management (user access, backup)

- To ensure the network is used safely.
- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet and email access using a unique USO (.302), audited username and password. A separate windows login is used to access the computer network.

- Has set-up the network so that users cannot download executable files/programmes. Users do not have administration rights to install software.
- Employs the network manager through Capita IT School Support Service who ensure their technicians are up-to-date with LGfL services and policies;
- Has set-up the network with a shared work or personal work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day. We request that they DO however switch the computers off at the end of the day.
- Maintains equipment to ensure Health and Safety is followed; e.g. equipment installed and annually checked by Capita IT Schools Support Service (PEAT)
- Has separate curriculum and administration networks. Access to Integris G2 Data system is set-up so as to ensure staff users can only access modules related to their role;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support or our Education Welfare Officers accessing attendance data on specific children;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

Passwords policy

Brunswick Park Primary & Nursery School

- Provides all pupils with their own unique (LGfL USO) username and password which gives them access to the network,;

- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

E-mail

CHBP

- Pupils are introduced to principles of e-mail through the Visual Mail facility in the London MLE OR closed 'simulation' software.
- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- Never use email to transfer staff or pupil personal data. We use secure systems: S2S (for school to school transfer) & USO-FX
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous e-mail addresses: office@brunswickpark.barnetmail.net for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively using the AutoUpdate facility to use up to date account details of users from the Integris G2 system.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

School website

- The school's public website includes some photographs of children but these are not linked to any children's names or personal information.
- The website includes up to date information on: ethos, admissions, performance, curriculum, policies, pupil premium allocation and contact details.

Social networking, blogs

- Social networking sites are not accessible from school and the school works hard to educate children, parents and staff about the risks involved.
- Parents are informed that Facebook and other social media should only be accessed by pupils over 13 years of age.

Video Conferencing

- CHBP only uses secure academic video conferencing facilities.

3. Data security

- All staff are eDBS checked and records are held in one single central record.
- Staff are required to use STRONG passwords for access into our Integris G2 system.
- Staff are required to change their passwords into Integris G2 and USO admin site, regularly and at least twice a year.
- Staff have a secure area on the network to store sensitive documents or photographs.
- Staff are required to log-out of the Integris G2 system when leaving their computer, but also enforce lock-out after 20 mins idle time.
- Staff know to report any incidents where data protection may have been compromised to the Data Protection Officer.
- We require that any data must be encrypted if it is to be removed from the school. We use automatically encrypted flash drives for this purpose and limit such data removal.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London USO FX system to transfer data within the LA.
- We use the LGfL secure data transfer for creation of online user accounts for access to broadband services and the London MLE, i.e. Atomwide's AutoUpdater.
- We store any paper based data in a locked storage office with restricted access.
- Our pupil data is held by secure online services.
- Weekly back-up of office data is completed using an encrypted external hard drive and held off-site.
- We ask staff to undertake at least annual house keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Data is removed from hard drives before disposal.

4. Equipment and Digital Content

Mobile phones:

- Personal mobile phones should be switched off and out of sight during teaching time.
- Staff should not use personal headphones whilst walking around the school building.
- In exceptional circumstances permission to use personal mobile phones may be obtained from the Executive Headteacher or Head of School.

Digital images and video:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;
- Digital images/video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- Staff may not take photos or video of pupils on their personal phones, cameras or other devices.
- We do not identify pupils in publicly available online photographs.

5. Education and Curriculum

Online Safety Curriculum

CHBP provides a flexible, relevant and engaging online safety curriculum in line with our computing curriculum – this is also shared with parents through informal coffee mornings. A key aim is to teach pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' online safety. We have core rules to help children including 'Stop and think before you click'.

- Pupils are taught a range of skills and behaviours appropriate to their age and experience, organised into 3 strands:
- Online research
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to know not to download any files – such as music files - without permission;

- Online communication and collaboration
    - to understand 'Netiquette' behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to have strategies for dealing with receipt of inappropriate materials;
- to understand why and how some people will 'groom' young people for inappropriate reasons;
- that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;

- Online publishing
    - how images can be manipulated and how to publish for a wide range of audiences which might include governors, parents or younger children;
    - to understand why they must not post pictures or videos of others without their permission;
    - to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Staff and governor training

- The computing lead will keep abreast of current legislation through regular training;
- All staff will receive annual training or updates in online safety in line with ;
- Governors will have access to regular training in online safety to support them with safeguarding responsibilities;

Parent awareness and training

- CHBP runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school website;
    - demonstrations, practical sessions held at school;
    - distribution of 'think u know' for parents materials
    - suggestions for safer internet use at home;
    - provision of information about national support sites for parents.

6. Expected Conduct and Incident management

- All staff sign our 'Staff Acceptable Use Agreement' (Appendix 1) to say they have read and understood the e-safety policy and guidance on handling e-safety incidents (Appendix 4).
- KS1 pupils sign the 'Think before you click' agreement (Appendix 2a) and KS2 pupils sign 'Acceptable use of technology Agreement' (Appendix 2b) to say they have read and understood the online safety rules, and we explain how any inappropriate use will be dealt with.
- Parents sign the online safety agreement (Appendix 3) giving permission for pupils to use ICT and online resources and for the school to use digital images for school purposes;
- The school will maintain an online safety incident log.

Content

- CHBP Federation fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material online that makes them feel uncomfortable;
- Staff must report any failure of the web filtering systems directly to the Designated Safeguarding Lead or SBM who will escalate as appropriate to Capita's IT Support or LGfL;
- Executive Headteacher must refer any material we suspect to be illegal to the appropriate authorities ie. Police and the LADO.
- Staff supervise pupils' use of the internet at all times;
- Staff always preview websites before use;
- Staff plan the curriculum content for internet use selecting appropriate websites and avoid open web-searching;
- CHBP Federation ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;

Conduct

- In accordance with our anti-bullying policy pupils are encouraged to tell a member of staff if there is a cyber-bullying incident;
- Staff should keep copies of any abusive material as evidence, tell the child not to respond and then follow the school anti-bullying policy for reporting;
- If it is a serious case involving threat or intimidation the Executive Headteacher or other member of the safeguarding team may need to report it to the police;
- If staff become aware that a child may have put themselves in a vulnerable position through their online behaviour (e.g. underage use of Facebook, uploading

videos to Youtube, contacting strangers online) it must be reported to the Designated Safeguarding Lead.

- If a staff member becomes aware of any inappropriate behaviour or use of digital technology by an adult in school, they must report it to the Designated Safeguarding Lead.

Appendix 1 -Brunswick Park School e-Safety Policy: Staff Acceptable Use Agreement (Digital technologies)

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email etc) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only not use the systems for inappropriate personal or recreational use.
- I will not disclose my username(s) or password(s) to anyone else, nor will I try to use any other person's username and password: if they reveal it to me and will advise them to change it. I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only use the approved, secure LGfL email system(s) for any school business.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published on the school website it will not be possible to identify by name, or other personal information, those who are featured.
- I will ensure that digital imagery/video posted on the MLE will be restricted to children whose parents have given permission.
- I will not use chat or social networking sites on school equipment or during the school day.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not use my personal mobile phone to communicate with parents unless permission has been given by the Executive Headteacher or Head of School in exceptional circumstances.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will not 'friend' pupils or parents on my private social networking site and will ensure my privacy settings prevent wider public accessing my personal profile.

The school is responsible for providing safe and secure access to technologies and ensure the smooth running of the school:

- I will embed the school's online safety curriculum into my teaching.
- I understand that my personal mobile phone/device must be switched off and out of sight during teaching time, unless express permission has been given by the Executive Headteacher/Head of School in exceptional circumstances.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will only transport personal information on the school encrypted data stick.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name	
Signed	
Date	

Appendix 2a – 'Think before you Click' agreement

Think Before you Click	
S 	**I will only use the Internet and email with an adult**
A 	**I will only click on icons and links when I know they are safe**
F 	**I will only send friendly and polite messages**
E 	**If I see something I don't like on a screen, I will always tell an adult**

Appendix 2b - KS2 Pupil Acceptable Use of Technology Agreement

For my own personal safety:

- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only e-mail people I know, or a responsible adult has approved.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will hand in my mobile phone to the office each morning.

I will act as I expect others to act towards me:

- I will only send or upload polite and sensible messages or images.
- I understand that nasty/hurtful messages would be considered as cyberbullying.
- I will not take or distribute images of anyone without their permission.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.

When using the internet for research:

- I will only use other people's writing, pictures, music or video if I know I have copyright permission.

Keeping our school system secure:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not attempt to visit internet sites that I know to be banned by the school.
- I will only use the school's computers for schoolwork and homework.
- I will not bring files into school without permission or upload inappropriate material to my workspace.

I have read and understand these rules and agree to them.

Signed: Date:

Appendix 3 - CHBP Online Safety Agreement Form: Parents

Internet and IT:
As the parent or legal guardian of the pupil named below, I grant permission for the school to give my child access to the internet at school, the school's education email system and IT facilities and equipment at the school.

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution, including monitoring and web filtering system to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video:

I understand that the school Online Safety Policy covers the use of digital images and video and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites:
I understand that the school Online Safety Policy covers the use of social networking and media sites and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

My child's name:
Parent / guardian signature: **Date:**

The Use of Digital Images and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your child.

We follow the following rules for any external use of digital images e.g. school's website:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used at school include:

- Your child being photographed as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent/guardian on Tapestry.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Staff are not allowed to take photographs or videos on their personal equipment.