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 of our community - this is an integral part of each school's culture and ethos. Policies are formulated and implemented with this in mind, placing the wellbeing of all at the forefront at all times.'

Online Safety Policy

MARCH 2023

1. Introduction and overview
    - Rationale and Scope
    - Roles and responsibilities
    - How policy be communicated to staff/pupils/community

2. Managing the ICT infrastructure
    - Internet access, security (virus protection) and filtering
    - Network management (user access, backup)
    - Passwords policy
    - E-mail
    - School website
    - Learning platform
    - Social networking
    - Video Conferencing

3. Data security

4. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

5. Education and Curriculum
    - Pupil e-safety Curriculum
    - Staff and governor training
    - Parent awareness and training

6. Expected Conduct and Incident management

Appendices:

1 Acceptable Use Agreement (Staff)

2a and 2b Acceptable Use Agreement (Pupils)

3 Acceptable Use Agreement including photo/video permission (Parents)

1. Introduction and Overview

Rationale
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. • 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.

Role	Key Responsibilities
	• 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 e-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' (See separate policy.) to say they have read and understood the e-safety policy and guidance on handling e-safety incidents.
- KS1 pupils sign the 'Think before you click' agreement (See separate policy.) and KS2 pupils sign 'Acceptable use of technology Agreement' (See separate policy.)

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 (See separate policy.) 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.