Chiswick & Bedford Park Preparatory School

E-Safety Policy

Introduction
The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Scope
This policy applies to all pupils, teaching staff, support staff, visitors and all volunteers at Chiswick & Bedford Park Preparatory School ("the School").
This policy works alongside the school's Safeguarding Policy and ensures all members of the school community are kept safe.

Aims
Our aims are to ensure that all pupils:

- Will use the internet and other digital technologies to support, extend and enhance their learning;
- Will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- Will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working; and
- Will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning. Pupils will be given clear objectives for internet use, web content will be subject to age-appropriate filters and internet use will be embedded in the curriculum.

Managing the Internet Safely

Technical and Infrastructure approaches
The School:

- Ensures network health through use of Sophos anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all KS2 users;
- Ensures filters have been set up to block the majority of chat room and Social Networking sites. This is checked on a regular basis as technology grows;
- Ensures that if children are to post anything online as part of their Digital Literacy work, it must first go to their Class Teacher to approve, before it will go 'live' onto the page;
- Has blocked pupil access to music download or shopping sites; and

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.

The School:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures staff report any concerns to either the ICT Coordinator or via IMIS;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- (Or uses the safe google image search such as kiddle.com).
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Co-ordinator or TurnItOn, who will deal with it appropriately;
- Requires pupils to individually sign an e-safety / acceptable use agreement form which is fully incorporated within the schools teaching and learning;
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy in the policies file;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the School;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in accordance with the School's Behaviour and Discipline Policy;
- Ensures designated safeguarding officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents;
- Parents are invited to our regular e-safety meetings to hear more about our e-safety policy. Refer to school website for more information on the next upcoming e-safety meeting.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

The School:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to put the monitor down and tell the teacher straight away. Teacher to report the URL to the appropriate body.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident; (refer to cyber bullying procedure)
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety curriculum throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - 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 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 how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - 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 understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;

- 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;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Provides relevant and up to date training on all aspects of e-safety, including:
    - Information on the School web site;
    - distribution of 'think u know' for parents materials
    - suggestions for safe Internet use at home

Cyber Bullying Procedure

Definition: Cyberbullying is the use of technology to bully an individual or a group with the intent to cause harm. The intended harm may be social, psychological and, in extreme cases, physical.

What does it look like: Cyberbullying can occur in a number of ways, including:

- abusive texts and emails
- hurtful messages, images or videos
- imitating others online
- excluding others online
- nasty online gossip and chat

Early Intervention:

- Encourage children and staff to report bullying incidents involving themselves or pupils.
- Classroom teachers and head teacher will, on a regularly reminding students and the school's staff to report incidents of bullying. Regular monitoring (by TIO) of student traffic on school's computer networks to identify potential problems will take place.
- Parents encouraged to contact school if they become aware of a problem

Intervention:

- Once identified each bully, victim and witnesses will be spoken with, and all incidents or allegations of bullying will be fully investigated and documented.
- Parents to be contacted.
- Pupils and staff identified by others as bullies will be informed of allegations.
- Both bullies and victims will be offered counselling and support.
- Access to the School's network and computers will be removed from cyber bullies for a period of time.
- If pupil bullying persists parents will be contacted and consequences implemented consistent with the school's Anti Bullying Policy

Additional Information

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.**

Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing will never be allowed. Pupils will use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.

Teachers will check websites before allowing pupils to use them. This is to ensure that the websites are age appropriate, do not contain any links to inappropriate sites, do not include downloads and are fit for purpose.

Teachers' web site selections for various topics can be put onto a topic page Google Classroom so pupils can access out of School, from home etc. Links to websites may be posted to Google Classroom; therefore, sites should always be previewed and checked by the Classroom Teacher.

Where possible, teachers will use QR codes to help direct students to the correct websites that have been deemed suitable.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search.
Google image search will be set-up to run in 'safe' mode although this is not fully without risk.
Teachers are encouraged to use search engines such as Kiddle that are specifically developed for children, implementing various levels of protection regular search engines do not have.
Pupils will be made aware of copyright and how this affects the use of images found on the internet.

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. The Google Apps for Education (GAFE) platform is used in years 3 – 6 and allows pupils to work collaboratively online, post constructive comments and suggestions. GAFE allows pupils to communicate with their teacher through a class stream that is only visible to other class members and those who have been invited by the Class Teacher.

Blogs: this is sometimes used as a method of online publishing, perhaps creating class blogs, or to creatively support a specific School project. A 'safe' blogging environment is likely to be part of GAFE and is controlled by the classroom teacher and TIO technician.
Google Apps for Education (GAFE) will be used interactively and collaboratively within certain

classroom settings. This will be a closed group, with only those granted access being able to take part in the project.

Webcams and Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project.

Video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom. For large group work high quality video conferencing hardware equipment is required to be plugged into the network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2. Advice can be found here http://www.lgfl.net/SERVICES/CURRICULUM/Pages/WeatherStations.aspx http://www.lgfl.net/learningresources/VideoConferencing/Pages/Home.aspx

Pupils will not have access to any webcams found through online searches. Classroom teachers will provide an approved link to a webcam, if this is deemed necessary for the classroom project. Pupils will be made aware of the dangers of 1:1 live web-chats conducted

Social Networking Sites

These are a popular aspect of the web for young pupils. Sites such as Facebook, Instagram, Snapchat and Youtube allow users to share and post web sites, videos, podcasts, etc. To sign up for these sites, an age limit of 13 is needed. No pupils are encouraged to sign up for any of these Sites. Pupils are made aware that these are public spaces for both children (13+) and adults. Pupils are informed of sites (such as YouTube for Kids, Moshi Monsters) that are designed specifically for children to social network in a safe environment, and give parents access to privacy settings.

Podcasts

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children are made aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area. No podcasts will be conducted without the direct supervision from a teacher. http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Google Apps for Education (GAFE)

Pupils from years 3 - 6 will have their own personal login to Google Apps for Education. Google Apps include:

- Docs
- Slides
- Sites
- Classroom
- Sheets

- Drive

Gmail will be disabled for all students.

Through these Apps, pupils have the ability to share their work with a member of the class, staff or family. The sharing of this work comes directly from the student and needs to be accepted by the person they are sharing with. Within the settings, pupils will ensure that their work cannot be shared by other people, thus closing the connection to the general public. This is a safe, monitored system for accessing, sharing, creating and storing documents on the cloud. Pupils will be taught how to gain the best educational benefits from this service while continuing to use safe practices.

Chatrooms

Pupils will be taught to understand the importance of safety within any chat room. Chat rooms will not be used in the School. The School cannot, however, limit a pupil's access to chat rooms outside of the School, where pupils are most at risk. Pupils will be made aware of the dangers surrounding the use of online chat within gaming platforms such as Minecraft. Pupils will be shown how to turn a chat feature off, block and report other users. All pupils are encouraged to tell an adult if they see anything they do not like online.

Sanctions and infringements

The School's Internet e-safety Policy is made available on the School website (www.cbppschool.co.uk) and explained to staff, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The School has clear possible sanctions for infringements.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on School computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Parents are invited to our regular e-safety meetings to hear more about this policy.

Date reviewed	**Date of next review**	**Date approved and agreed by Proprietors**
August 2019	**August 2020**	**August 2019**