E-Safety Policy

Ratified by Governors: November 2016
Review Date: November 2017
Member of Staff Responsible: Fateh Singh

1. Introduction and Overview

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Bush Hill Park Primary School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for BHP Primary School.

> *"Digital technologies are an important (but not dominant) part of children's lives. Even though children love playing digital games or watching videos, they also enjoy performing other non-digital activities. Digital technology use is balanced with many other activities, including outdoor play and non-digital toys."*
>
> *Research Highlights for Children's Online Safety #81 June, 2015*

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

The school's e-safety coordinator is Mr Singh. The e-safety Policy and its implementation shall be reviewed annually. It was approved by the Governors and will be reviewed in the winter term 2016 as part of our safeguarding review.

2. Roles and Responsibilities

Governors:	Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will include: ✓ Regular meetings with the e-Safety Coordinator/Officer. ✓ Regular monitoring of e-safety incident logs. ✓ Reporting to the Behaviour & Safety Committee.
Headteachers and Senior Leaders:	✓ The Headteachers are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator. ✓ The Headteachers/Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. ✓ The Headteachers/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. ✓ The Headteachers and Assistant Heads should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Co-ordinator:	✓ Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents. ✓ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. ✓ Provides training and advice for staff. ✓ Liaises with school ICT technical staff. ✓ Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
Teachers and support staff	✓ Be able to log issues ✓ Understand the key ethos to issues in regards to esafety ✓ Keep up to date with school policy and procedures ✓ Attend staff insets and meetings

3. Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- ✓ The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- ✓ Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- ✓ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ✓ As part of the new Computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- ✓ The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-Ethnic society. We also measure and assess the impact regularly through meetings our SEN coordinator and individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Our school also participates in termly surveys, where students are given questions in regards to their Internet usage. This data is then feedback to the Senior Leadership Team and parents of those participating year groups. With this data we are able to proactivity act on any concerns and help with our future E-Safety lesson/workshop plans.

4. Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- ✓ All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- ✓ Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- ✓ Only authorised equipment, software and Internet access can be used within the school.

In addition to authorised access, LGFL (John Jackson, LGfL CEO, 07/16) have strongly advised against using search engines such as yahoo and google as it breaches their web based monitor tools – see https://www.lgfl.net/online-safety/google.aspx for full details. As a result the entire student network and no access to google, yahoo or YouTube to ensure our children are protected and thus we can monitor their activity.

5. World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- ✓ If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident via Scholar Pack this will be reviewed termly.
- ✓ The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- ✓ Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- ✓ The school will work in partnership with London Grid for Learning (LGFL) to ensure filtering systems are as effective as possible.

6. E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- ✓ Pupils may only use approved e-mail accounts on the school website.
- ✓ Pupils must immediately tell a teacher if they receive offensive e-mail.
- ✓ Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- ✓ Whole class or group e-mail addresses should be used in school rather than individual addresses.
- ✓ Access in school to external personal e-mail accounts is not allowed.
- ✓ E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- ✓ Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

7. Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

8. Social Networking

- ✓ Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- ✓ Use of social networking sites and newsgroups in the school, is not allowed and will be monitored.
- ✓ Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- ✓ Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- ✓ Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
    - o Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

9. Reporting

- ✓ All breaches of the e-safety policy need to be recorded on Scholar Pack via the E-Safety tab. The details of the user, date and incident should be reported.
- ✓ Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.
- ✓ Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT in the same day.
- ✓ Allegations involving staff should be reported to the Headteachers.
- ✓ Evidence of incidents must be preserved and retained.
- ✓ The curriculum will cover how pupils should report incidents e.g. CEOP button now on our school website, trusted adult and Childline.

10. Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- ✓ Pupils by permission of the Head teacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- ✓ The sending of abusive or inappropriate text messages is forbidden.
- ✓ Staff should always use the school phone to contact parents.
- ✓ Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should

ensure that their phones are turned off and stored safely away during the teaching day.

- ✓ Staff may use their mobile phones in the staffroom/one of the school offices.
- ✓ Parents cannot use mobile phones on school trips to take pictures of the children

On trips staff mobiles are used for emergency only.

11. Digital/Video Cameras/Photographs/IPads

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- ✓ Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- ✓ Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- ✓ Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- ✓ One of the Headteachers or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- ✓ Staff should always use a school camera to capture images and should not use their personal devices.
- ✓ Photos taken by the school are subject to the Data Protection act.

12. Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- ✓ Contact details on the Website will be the school address, e-mail and telephone number.
- ✓ Staff and pupils' personal information will not be published.
- ✓ One of the Headteachers or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- ✓ Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- ✓ Pupils' full names will not be used in association with photographs.
- ✓ Consent from parents will be obtained before photographs of pupils are published on the school Website.
- ✓ Work will only be published with the permission of the pupil.
- ✓ Parents should only upload pictures of their own child/children onto social networking sites.

- ✓ The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

13. Information System Security

- ✓ School ICT systems capacity and security will be reviewed regularly.
- ✓ Virus protection will be installed and updated regularly.
- ✓ Security strategies will be discussed with the LGFL.
- ✓ E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

14. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

15. Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

16. Handling E-Safety Complaints

- ✓ Complaints of Internet misuse will be dealt with by a senior member of staff.
- ✓ Any complaint about staff misuse must be referred to one of the Headteachers.
- ✓ Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- ✓ Pupils and parents will be informed of the complaints procedure.
- ✓ Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

17. Communication of Policy

Pupils:

- ✓ Rules for Internet access will be posted in all computer suites.
- ✓ Pupils will be informed that Internet use will be monitored.
- ✓ Pupils will be informed of the importance of being safe on social networking sites such as msn/Facebook. This will be strongly reinforced across all year groups during computing/ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

17.1 Staff:

All staff will be given the School e-safety Policy and its importance explained.

17.2 Parents:

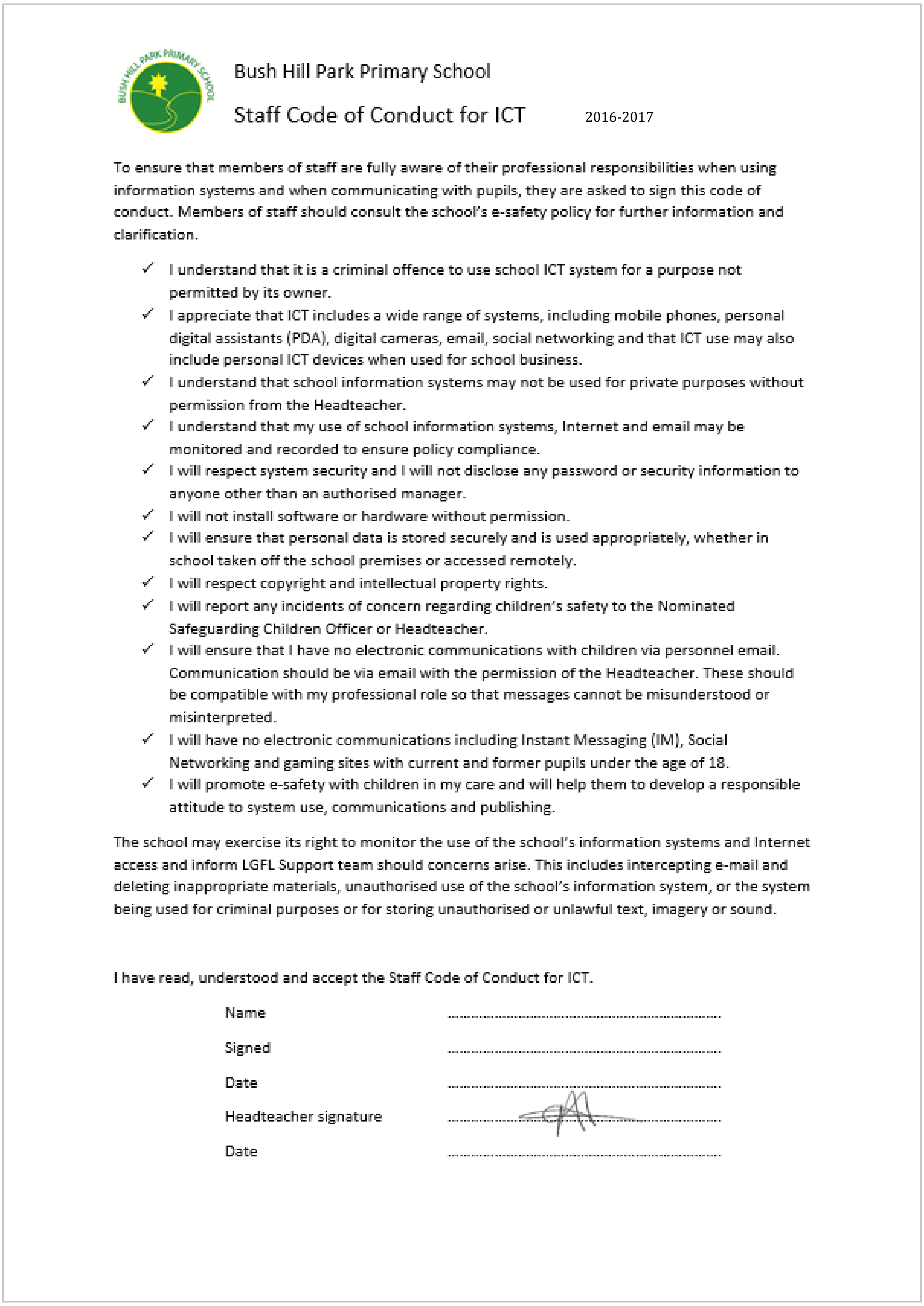
Parents' attention will be drawn to the School e-safety Policy on the school Website. We will continue to run designated workshops for parents to feedback information from data collected from Point 3.

17.3 Further Resources

We have found these web sites useful for e-safety advice and information.

www.thinkuknow.co.uk	Set up by the Police with lots of information for parents and staff including a place to report abuse.
www.childnet-int.org	Non-profit organisation working with others to "help make the Internet a great and safe place for children".
www.commonsensemedia.org	With fun apps and games, learning can happen anywhere. Our independent ratings help you find the best.
vodafonedigitalparenting.co.uk	Online digital magazine that guides parents on best practices with their children when using computers.
saferinternet.org.uk	Non-profit organization, with resources & advice

18. Appendix 1 Staff ICT Code of Conduct



Bush Hill Park Primary School

Staff Code of Conduct for ICT 2016-2017

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- ✓ I understand that it is a criminal offence to use school ICT system for a purpose not permitted by its owner.
- ✓ I appreciate that ICT includes a wide range of systems, including mobile phones, personal digital assistants (PDA), digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- ✓ I understand that school information systems may not be used for private purposes without permission from the Headteacher.
- ✓ I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- ✓ I will respect system security and I will not disclose any password or security information to anyone other than an authorised manager.
- ✓ I will not install software or hardware without permission.
- ✓ I will ensure that personal data is stored securely and is used appropriately, whether in school taken off the school premises or accessed remotely.
- ✓ I will respect copyright and intellectual property rights.
- ✓ I will report any incidents of concern regarding children's safety to the Nominated Safeguarding Children Officer or Headteacher.
- ✓ I will ensure that I have no electronic communications with children via personnel email. Communication should be via email with the permission of the Headteacher. These should be compatible with my professional role so that messages cannot be misunderstood or misinterpreted.
- ✓ I will have no electronic communications including Instant Messaging (IM), Social Networking and gaming sites with current and former pupils under the age of 18.
- ✓ I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access and inform LGFL Support team should concerns arise. This includes intercepting e-mail and deleting inappropriate materials, unauthorised use of the school's information system, or the system being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Name ....

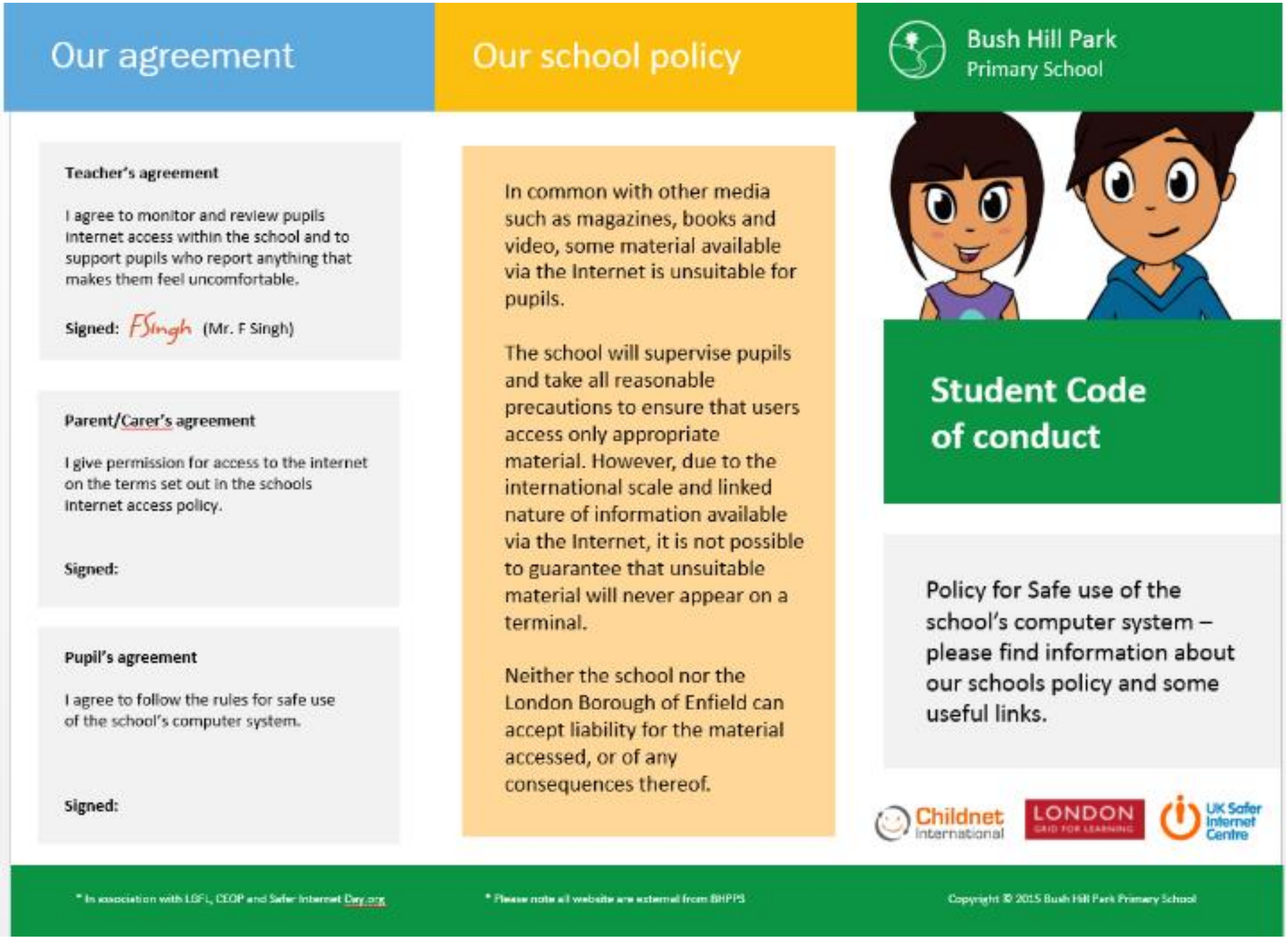
Signed ....

Date ....

Headteacher signature ....

Date ....

18.1 Appendix 2 Student Code of Conduct



Our agreement

Teacher's agreement

I agree to monitor and review pupils internet access within the school and to support pupils who report anything that makes them feel uncomfortable.

Signed: FSingh (Mr. F Singh)

Parent/Carer's agreement

I give permission for access to the internet on the terms set out in the schools internet access policy.

Signed:

Pupil's agreement

I agree to follow the rules for safe use of the school's computer system.

Signed:

Our school policy

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.

The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due 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 on a terminal.

Neither the school nor the London Borough of Enfield can accept liability for the material accessed, or of any consequences thereof.

Bush Hill Park
Primary School

Student Code of conduct

Policy for Safe use of the school's computer system – please find information about our schools policy and some useful links.

Childnet International

LONDON GRID FOR LEARNING

UK Safer Internet Centre

* In association with LGFL, CEOP and Safer Internet Day.org

* Please note all website are external from BHPPS

I will keep my school safe

- ✓ I will only access the system with my class login.
- ✓ I will only use the computers for school work and homework.
- ✓ I will not bring Mobile phones, USB keys, MP3 players, hand held games devices or other removable media into school unless I have been given permission.

I will be fair to others

- ✓ I will only email people I know, or my teacher has approved. The messages I send will be polite and sensible.
- ✓ I will not access other people's files. I will always ask permission before printing.
- ✓ I understand that the school may check my computer files and may monitor the Internet sites I visit.
- ✓ I will not post inappropriate messages or images about others on ANY form of social media..

I will keep myself safe

- ✓ I will ask permission from a member of staff before using the Internet.
- ✓ I will not give my home details or arrange to meet someone unless my parent, carer or teacher has given permission.
- ✓ To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- ✓ I will keep my personal login details safe and not share them with others.

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.