Dated September 2016

Islamia Girls School/Brondesbury College "The School"

e-Safety Policy

CONTENTS

1. Why does Islamia Schools Limited (ISL) need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of School. It includes education for all members of the School community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Our School must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider School community. It is crucial that all members of the School community are aware of the offline consequences that online actions can have.

We must be aware of our legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and ISL.

The e-Safety policy is essential in setting out how Islamia Schools Ltd plans to develop and establish our e-Safety approach and to identify core principles which all members of the School community need to be aware of and understand.

The School e-Safety Coordinator is: **Mr. S. Yousaf (BC) / Mrs Khalladi (IGS)**

Policy approved by Head Teacher: **Mr. A. Ali (BC) / Mrs S Jabeen (IGS)**

Date: 10/11/2015

Policy approved by School Committee: …….. (Chair of Committee)

Date: …….....

2. Teaching and Learning

2.1 Why is Internet use important?

- 2.1.1 Internet use is part of the statutory curriculum and is a necessary tool for learning
- 2.1.2 The Internet is a part of everyday life for education, business and social interaction
- 2.1.3 The School has a duty to provide students with quality Internet access as part of their learning experience
- 2.1.4 Students use the Internet widely outside School and need to learn how to evaluate Internet information and to take care of their own safety and security
- 2.1.5 The purpose of Internet use in School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions
- 2.1.6 Internet access is an entitlement for students who show a responsible and mature approach to its use

2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- 2.2.1 Access to worldwide educational resources including museums and art galleries
- 2.2.2 Inclusion in the National Education Network which connects all UK Schools
- 2.2.3 Educational and cultural exchanges between students worldwide
- 2.2.4 Vocational, social and leisure use in libraries, clubs and at home
- 2.2.5 Access to experts in many fields for students and staff
- 2.2.6 Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- 2.2.7 Collaboration across networks of Schools, support services and professional associations
- 2.2.8 Improved access to technical support including remote management of networks and automatic system updates
- 2.2.9 Exchange of curriculum and administration data with Brent and DfE
- 2.2.10 Access to learning wherever and whenever convenient

2.3 How can Internet use enhance learning?

- 2.3.1 The School's Internet access will be designed to enhance and extend education
- 2.3.2 Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- 2.3.3 The Schools will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law
- 2.3.4 Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students
- 2.3.5 Staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability

2.3.6 Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.3.7 Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

2.4 How will students learn how to evaluate Internet content?

2.4.1 Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy as part of the computer science curriculum

2.4.2 Students will use age-appropriate tools to research Internet content

2.4.3 The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-School requirement across the curriculum

3. Managing Information Systems

3.1 How will information systems security be maintained?

3.1.1 Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive
- Users must take responsibility for their network use
- Workstations should be secured against user mistakes and deliberate actions
- Servers must be located securely and physical access restricted
- The server operating system must be secured and kept up to date
- Virus protection for the whole network must be installed and current
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption

3.1.2 Wide Area Network (WAN) security issues include:

- The security of the School information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan
- Unapproved software will not be allowed in work areas or attached to email
- Files held on the School's network will be regularly checked
- The ICT coordinator/network manager will review system capacity regularly
- The use of user logins and passwords to access the School network will be enforced

3.2 How will email be managed?

3.2.1 Students may only use approved email accounts for School purposes

3.2.2 Students must immediately tell a designated member of staff if they receive offensive email

3.2.3 Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult

3.2.4 Staff will only use official School provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team

3.2.5 Access in School to external personal email accounts may be blocked, if necessary

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

3.2.7 Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on School headed paper would be

3.2.8 The forwarding of chain messages is not permitted

3.2.9 Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff

3.2.10 Staff should not use personal email accounts for professional purposes

3.3 How will published content be managed?

3.3.1 The contact details on the website should be the School address, email and telephone number. Staff or students' personal information must not be published

3.3.2 Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT')

3.3.3 The head teacher will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate

3.3.4 The School website will comply with the School's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

3.4 Can students' images or work be published?

3.4.1 Images or videos that include students will be selected carefully and will not provide material that could be reused

3.4.2 Students' full names will not be used in association with photographs

3.4.3 Written permission from parents or carers will be obtained before images/videos of students are electronically published

3.4.4 Students work can only be published with their permission or the parents

3.4.5 The School will have a policy regarding the use of photographic images of children which outlines policies and procedures

3.5 How will social networking, social media and personal publishing be managed?

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

3.5.1 The School will control access to social media and social networking sites

3.5.2 Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

3.5.3 Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom

3.5.4 Staff official blogs or wikis should be password protected and run from the School website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis

3.5.5 Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the School where possible

3.5.6 Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private

3.5.7 All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory

3.5.8 Newsgroups will be blocked unless a specific use is approved

3.5.9 Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of School) will be raised with their parents/carers, particularly when concerning students' underage use of sites

3.5.10 Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the School Acceptable Use Policy

3.6 How will filtering be managed?

Access controls fall into several overlapping types (commonly described as filtering):

3.6.1 Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day

3.6.2 A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of content

3.6.3 Dynamic content filtering examines web page content or email for unsuitable words

3.6.4 Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold

3.6.5 URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate student access

3.6.6 Key loggers record all text sent by a workstation and analyse it for patterns

3.6.7 The School's broadband access will include filtering appropriate to the age and maturity of students

3.6.8 The School will work with the Schools Broadband team to ensure that filtering policy is continually reviewed

3.6.9 The School will have a clear procedure for reporting breaches of filtering. All members of the School community (all staff and all students) will be aware of this procedure

3.6.10 If staff or students discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate

3.6.11 changes to the School filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team

3.6.12 The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective

3.6.13 Any material that the School believes is illegal will be reported to appropriate agencies such as the police

3.6.14 The School's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers

3.7 How will videoconferencing be managed?

3.7.1 All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer

3.7.2 External IP addresses will not be made available to another site

3.7.3 Videoconferencing contact information will not be put on the School Website

3.7.4 The equipment must be secure and if necessary locked away when not in use

3.7.5 School videoconferencing equipment will not be taken off School premises without permission

3.7.6 Responsibility for the use of the videoconferencing equipment outside School time will be established with care

Users

- Students will ask permission from a teacher before making or answering a videoconference call.

- Videoconferencing will be supervised appropriately for the students' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-School site it is important to check that they are delivering material that is appropriate for your class.

3.8 How are emerging technologies managed?

3.8.1 Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for effective and safe practice in classroom use to be developed. Access will be denied until a risk assessment has been completed and safety has been established.

3.8.2 Virtual online classrooms and communities widen the geographical boundaries of learning. Online communities can also be one way of encouraging a disaffected student to keep in touch.

3.8.3 The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This is not easy, as authentication beyond the School may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

3.8.4 Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

3.8.5 New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or

personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a student using a phone to video a teacher's reaction in a difficult situation.

3.9 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

3.10 Students will be instructed about safe and appropriate use of personal devices. The School currently has a blanket ban on personal Smart phones and smart devices for students. Students only have access to the internet via the School's computers. Non-smart phones can be brought in to School but must be handed in to the reception on entry and picked up before exiting.

3.11 How should personal data be protected?

3.11.1 The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

3.11.2 Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

3.11.3 The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4. Policy Decisions

4.1 How will Internet access be authorised?

4.1.1 The School will maintain a current record of all staff and students who are granted access to the School's electronic communications.

4.1.2 Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.

4.1.3 When considering access for vulnerable members of the School community (such as with children with special education needs) the School will make decisions based on the specific needs and understanding of the student(s).

4.2 How will risks be assessed?

4.2.1 The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. The School cannot accept liability for the material accessed, or any consequences resulting from Internet use.

4.2.2 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.

4.2.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the local police.

4.2.4 Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 How will the School respond to any incidents of concern?

4.3.1 All members of the School community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content, radicalisation etc.)

4.3.2 The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

4.3.3 The Designated Child Protection (designated Safeguarding Lead DSL and SPOC) Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

4.3.4 The School will manage e-Safety incidents in accordance with the School discipline/ behaviour policy where appropriate.

4.3.5 The School will inform parents/carers of any incidents of concerns as and when required.

4.3.6 After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required.

4.3.7 Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police

4.3.8 If the School is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Students Officer who will seek advice from the Brent LSCB e-Safety Officer.

4.4 How is the School dealing with the online threat of radicalisation and preventing extremism?

4.4.1 Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences. Brent Council provides interventions under the Channel project which is part of the government's Prevent strategy to divert young people away from extremism which are provided by the Integrated Youth Support Services. In incidents of this kind will be dealt with under the School's safeguarding and child protection policy. This policy covers the procedures involved in dealing with radicalisation and extremism.

4.4.2 Students are warned of the risks during the e safety workshops as well as morning assemblies, ICT lessons and IPSHE.

4.4.3 Social networking sites are blocked. Students currently can only access email accounts.

4.4.4 Some other websites have also been blocked. This list is being regularly updated and is kept with the IT manager of the Schools.

4.4.5 The e-safety contact officer /co-ordinator should record and review any incidents in order to establish whether there are any patterns of extremist groups targeting the service. This should be discussed with the Head Teacher who is also the SPOC, who will make the relevant contact with Brent Family Front Door.

4.4.6 If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, staff should refer the student to the School's Designated Safeguarding Lead. The designated safeguarding lead will do an initial assessment with the other DSLs in the School and refer the student to the Brent Officer, Kibibi Octave.

4.5 How will e–Safety complaints be handled?

4.5.1 Complaints about Internet misuse will be dealt with under the School's complaints procedure.

4.5.2 Any complaint about staff misuse will be referred to the head teacher.

4.5.3 All e–Safety complaints and incidents will be recorded by the School, including any actions taken.

4.5.4 Students and parents will be informed of the complaints procedure.

4.5.5 Parents and students will need to work in partnership with the School to resolve issues.

4.5.6 All members of the School community will need to be aware of the importance of confidentiality and the need to follow the official School procedures for reporting concerns.

4.5.7 Discussions will be held with the Brent Children's Safeguard Team to establish procedures for handling potentially illegal issues.

4.5.8 Any issues (including sanctions) will be dealt with according to the School's disciplinary, behaviour and child protection procedures.

4.5.9 All members of the School community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the School community.

4.6 How is the Internet used across the community?

4.6.1 The School will liaise with local organisations to establish a common approach to e–Safety.

4.6.2 The School will be sensitive to Internet-related issues experienced by students out of School, e.g. social networking sites, and offer appropriate advice.

4.6.3 The School will provide appropriate levels of supervision for students who use the internet and technology whilst on the School site.

4.6.4 The School will provide an AUP for any guest who needs to access the School computer system or internet on site.

4.7 How will Cyber bullying be managed?

4.7.1 Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

4.7.2 Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

4.7.3 It is essential that young people, School staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

4.7.4 Section 89 of the Education and Inspections Act 2006:

4.7.4.1 every School must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the School's behaviour policy which must be communicated to all students, School staff and parents

4.7.4.2 gives Head Teachers the ability to ensure that students behave when they are not on School premises or under the lawful control of School staff

4.7.5 Cyber bullying (along with all other forms of bullying) of any member of the School community will not be tolerated. Full details are set out in the School's policy on anti-bullying and behaviour.

4.7.6 There are clear procedures in place to support anyone in the School community affected by cyberbullying.

4.7.7 All incidents of cyberbullying reported to the School will be recorded.

4.7.8 There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

4.7.9 Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

4.7.10 The School will take steps to identify the bully, where possible and appropriate. This may include examining School system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

4.7.11 Students, staff and parents/carers will be required to work with the School to support the approach to cyberbullying and the School's e-Safety ethos.

4.7.12 Sanctions for those involved in cyberbullying may include:

4.7.12.1 The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

4.7.12.2 Internet access may be suspended at School for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the Schools anti-bullying, behaviour policy or Acceptable Use Policy.

4.7.12.3 Parent/carers of students will be informed.

4.7.12.4 School's behaviour policy will be applied.

4.7.12.5 The Police will be contacted if a criminal offence is suspected.

4.8 How will mobile phones and personal devices be managed?

4.8.1 Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

4.8.2 However, mobile phones can present a number of problems when not used appropriately:

4.8.2.1 They are valuable items which may be stolen or damaged;

4.8.2.2 Their use can render students or staff subject to cyberbullying;

4.8.2.3 Internet access on phones and personal devices can allow students to bypass School security settings and filtering.

4.8.2.4 They can undermine classroom discipline as they can be used on "silent" mode;

4.8.2.5 Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to

inappropriate capture, use or distribution of images of students or staff.

4.8.3 The use of mobile phones on site is not permitted for students. Students are required to hand in their mobile phones at the reception when entering the School and picked up at the end of School day when returning home. Smart phones and internet enabled devices are not permitted on site.

4.8.4 The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the School discipline/behaviour policy.

4.8.5 School staff will confiscate a phone or device if it found on site or with a student. The phone or device might be searched by the Senior Leadership team with the consent of the student or parent/carer if necessary to carry out any investigations related to contravention of the behaviour policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

4.8.6 Student Personal devices (non internet enabled) will not be used during lessons or formal School time. They should be switched off at all times.

4.8.7 Electronic devices of all kinds that are brought in to School are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

5 Students Use of Personal Devices

5.1 If a student breaches the School policy, then the phone or device will be confiscated and will be held in a secure place in the School office. Mobile phones and devices will be released to parents/carers in accordance with the School policy.

5.2 Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

5.3 If a student needs to contact his/her parents/carers they will be allowed to use a School phone. Parents are advised not to contact their child via their mobile phone during the School day, but to contact the School office.

5.4 Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

6 Staff Use of Personal Devices

6.1 Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

6.2 Staff will be issued with a School phone where contact with students or parents/carers is required.

6.3 Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

6.4 If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.

6.5 Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.

6.6 If a member of staff breaches the School policy, then disciplinary action may be taken.

7 Communication Policy

7.1 How will the policy be introduced to students?

7.1.1 Useful e–Safety programmes include:

7.1.1.1 Think U Know: www.thinkuknow.co.uk

7.1.1.2 Childnet: www.childnet.com

7.1.1.3 Kidsmart: www.kidsmart.org.uk

7.1.1.4 Safe: www.safesocialnetworking.org

7.1.2 All users will be informed that network and Internet use will be monitored.

7.1.3 An e–Safety workshop will be established across the School to raise the awareness and importance of safe and responsible internet use amongst students. These workshops are run for parents and students.

7.1.4 Student instruction regarding responsible and safe use will precede Internet access.

7.1.5 e–Safety modules are included in the ICT curriculum covering both safe School and home use.

7.1.6 e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.

7.1.7 Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

7.1.8 Particular attention to e-Safety education will be given where students are considered to be vulnerable.

7.2 How will the policy be discussed with staff?

7.2.1 The e–Safety Policy will be formally provided to and discussed with all members of staff.

7.2.2 Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

7.2.3 Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

7.2.4 Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

7.2.5 The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.

7.2.6 All members of staff will be made aware that their online conduct out of School could have an impact on their role and reputation within School. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

7.3 How will parents' support be enlisted?

7.3.1 Parents' attention will be drawn to the School e–Safety Policy in newsletters and on the School website.

7.3.2 A partnership approach to e-Safety at home and at School with parents will be encouraged. This will include an e safety workshop for parents annually.

7.3.3 Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

7.3.4 Information and guidance for parents on e–Safety will be made available to parents.

7.3.5 Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

7.3.6 Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section".

APPENDIX 1
e-Safety Contacts and References

- **CEOP** (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- **Brent Local Safeguarding Children's Board:** http://www.brentlscb.org.uk/index.php
- **Childline:** www.childline.org.uk
- **Childnet:** www.childnet.com
- **Click Clever Click Safe Campaign:** http://clickcleverclicksafe.direct.gov.uk
- **Cybermentors:** www.cybermentors.org.uk
- **Digizen:** www.digizen.org.uk
- **Internet Watch Foundation** (IWF): www.iwf.org.uk
- **Kidsmart**: www.kidsmart.org.uk
- **Teach Today:** http://en.teachtoday.eu
- **Think U Know website**: www.thinkuknow.co.uk
- **Virtual Global Taskforce** — Report Abuse: www.virtualglobaltaskforce.com