Cannon Lane Primary School

E-Safety Policy

Date reviewed by staff: January 2016

Date approved by the Governing Body: January 2016

Date for review: Spring 2017

Rationale

At Cannon Lane Primary School, we are committed to ensuring the safety of our children and staff at all times. This policy is designed to ensure the online safety of all Cannon Lane Primary School children and staff in addition to providing help and support to parents and carers. The policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Cannon Lane Primary School will manage incidents that transgress this policy in conjunction with the school's Behaviour Policy(2016), Safeguarding Policy (2015) and Acceptable Use Agreement (2015).

Cannon Lane Primary School is a Rights Respecting school. The E-Safety Policy is underpinned by the United Nations Convention on the Rights of the Child. (http://www.unicef.org/crc/index_30160.html)

- **Article 17:** Every child has the right to reliable information from the media. This should be information that children can understand. Governments must protect children from materials that could harm them.
- **Article 34**: Governments should protect children from all forms of sexual exploitation and abuse. This provision in the Convention is augmented by the Optional Protocol on the sale of children, child prostitution and child pornography.
- **Article 36:** Children should be protected from any activity that takes advantage of them or could harm their welfare and development

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-safety incidents and monitoring reports. The role of the E-Safety Governor will include:

- regular contact with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs

Headteacher and Senior Leadership Team:
The Headteacher has a duty of care 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 Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:

- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school's E-Safety policy
- 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 Harrow Local Authority
- liaises with school technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments
- liaises with Governor responsible for to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

Technical staff are responsible for ensuring that**:**

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- school meets required e-safety technical requirements and any Harrow Local Authority or statutory guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection procedure, in which passwords are regularly changed.
- filtering is applied and updated on a regular basis .
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to E-Safety Co-ordinator and Headteacher.
- that monitoring software / systems are implemented and updated as agreed in school.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school / E-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-Safety procedures are embedded at the beginning of each academic year.
- children understand and follow the E-safety and acceptable use policies.
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that children know what to do if they encounter something inappropriate.

Children are responsible for:

- using the school digital technology systems in accordance with the Pupil Acceptable Use agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand procedures for the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national / local E-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Cannon Lane Primary School will also offer information and training sessions for parents and carers. Parents/carers may also wish to refer to relevant web sites / publications eg:

www.saferinternet.org.uk

http://www.childnet.com/parents-and-carers

www.ceop.police.uk

Education

Children
The Computing curriculum is presented within the Cannon Lane Primary School Computing Policy. The E-Safety policy compliments the Computing Policy by providing specific guidance on what children should learn in order to remain safe online. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the Computing/PSHE curriculum and staff should reinforce E-Safety messages across the Computing/PSHE curriculum. E-Safety issues should be regularly revisited throughout the academic year with children through Computing and PSHE lessons. Children should be taught to acknowledge the source of information

used in any curriculum subject and to respect copyright when using material accessed on the internet.

Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. It is accepted that from time to time, for good educational reasons, children may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be logged with those sites returned to the filtered list following the completion of the learning activity.

Education & Training – Staff / Volunteers

It is essential that all staff receive E-Safety training and understand their responsibilities. Training will be offered as follows:

- a planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly.
- all new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and any updates will be presented to and discussed by staff in staff INSET.
- The E-Safety Co-ordinator will provide advice / guidance / training to individuals as required.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Cannon Lane Primary School informs and educates children about these risks:

- children are informed and educated about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing,

distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff must not be used for such purposes.

- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website.
- Children's work can only be published with the permission of the child and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Cannon Lane Primary School will ensure that:

- we will hold the minimum personal data necessary to enable it to perform its function and we will not hold it for longer than necessary for the purposes it was collected for.
- every effort will be made to ensure that data held is accurate, up to date and that in accuracies are corrected without unnecessary delay.
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- we have a Data Protection Policy.
- we are registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- risk assessments are carried out.
- we have clear and understood arrangements for the security, storage and transfer of personal data.
- data subjects have rights of access and there are clear procedures for this to be obtained.
- there are clear and understood policies and routines for the deletion and disposal of data.
- there is a policy for reporting, logging, managing and recovering from information risk incidents.
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff at Cannon Lane Primary School must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When using communication technologies Cannon Lane Primary School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and children should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the E-Safety Co-ordinator – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and children or parents / carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Children are taught about E-Safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Cannon Lane Primary School has a duty of care to provide a safe learning environment for children and staff. Reasonable steps to prevent predictable harm must be in place.

Cannon Lane Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions.

  School staff should ensure that:
- No reference should be made in social media to children, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Social media is a very powerful means of sharing celebrations and social events among parents and carers. Cannon Lane Primary School recognises the importance of parents' communication with each other and the value that has for our school community. Cannon Lane Primary School would encourage parents to use social media positively. Any concerns or complaints should always be directed to the school office for resolution with school staff.

Responding to incidents of misuse

Cannon Lane Primary School a clear Safeguarding policy and a Behaviour policy which will be adhered to in the event of any incidents of misuse or contraventions of this policy by children or staff. If there is concern that illegal activity has taken place, this will be reported immediately to the police. It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- have more than one senior member of staff involved in this process with E-Safety co-ordinator. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material

- other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for Cannon Lane Primary School and possibly the Police and demonstrate that visits to these sites were carried out for child protection purposes.