PLAISTOW + KIRDFORD

PRIMARY SCHOOL

Plaistow & Kirdford Primary School
E-Safety Policy

Approved by:	Governing Body
Approval Date:	Nov 2015
To be reviewed:	Autumn 2018

Policy Overview:

This policy applies to all members of the school community (including staff, pupils / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school Computing 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 pupils / pupils 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

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. Governors will receive a termly update regarding E-Safety from the E-Safety Leader (Ross Harrision).

Headteacher / Senior Leaders:

• 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 Computing Leader
• The Headteacher and (at least) another member of the Senior Leadership Team 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. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
• The Headteacher is responsible for ensuring that the all other staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
• The Headteacher 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 Senior Leadership Team will receive monitoring reports from the Computing Subject Leader

E-Safety Coordinator/Computing Leader:

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and procedures
• 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 and sources training and advice for staff
• liaises with school's ICT technician
• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
• reports regularly to Senior Leadership Team

IT Network Manager:

The schools network is managed externally in terms of security and filtering by CAPITA through a Service Level Agreement negotiated by the Local Authority.

The ICT Technician is able to update web filters as a result of any e-safety concern.

Teaching and Support Staff:

All staff are responsible for ensuring that:

• they have an up to date awareness of e-safety matters and of the current Plaistow & Kirdford Primary School e-safety policy and practices
• they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP) – completed at staff induction

• they report any suspected misuse or problem to the Headteacher or Computing Leader for investigation/action
• all digital communications with pupils and parents/carers should be on a professional level and only should (ideally) be sent via the office email account. No school or pupil related communication should be sent from a personal email account.
• e-safety issues are embedded in all aspects of the curriculum and other activities
• pupils understand and follow the e-safety class charter and acceptable use policies
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• staff monitor the use of digital technologies, mobile devices (iPads, laptops) 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, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
. all use of social media is kept professional and does not bring the school into disrepute.

Child Protection Officer:

The Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

• sharing of personal data
• access to illegal/inappropriate materials
• inappropriate on-line contact with adults/strangers
• potential or actual incidents of grooming
• cyber-bullying

Pupils:

• are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
• 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
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, letters, home-school diaries and the school's website, www.plaistowandkirdfordprimaryschool.co.uk. Parents and carers will be encouraged to support Plaistow & Kirdford Primary School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

• digital and video images taken at school events
• children should not be bringing an device to school that allows them access to the internet. Children should be aware that even if a device such as a kindle or e-reader is subject to monitoring to ensure that appropriate content is being used.

Policy Statements

Education –pupils:

We as a staff understand that the technical element of E-Safety is only one element to ensuring the children in school are E-Safe. Through embedding E-Safety reminders and teaching points in to our everyday curriculum children are aware of the need to be safe online. The E-Safety curriculum is embedded as an essential part of our computing curriculum and should be visited by every teacher/staff member each time an electronic device is used.

- A planned e-safety thread through the curriculum is provided as part of Computing and all other lessons involving the internet and should be regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and class activities e.g. Anti-bullying Week, Internet Safety Day, Childline Visits
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Education – Parents/Carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

□ Home-school diaries
□ Newsletters
□ The E-Safety section on the school’s website–www.plaistowandkirdfordprimaryschool.co.uk
□ Parent workshop evenings / sessions
□ High profile events / campaigns e.g. Safer Internet Day – 9th February 2016
□ Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The computing lead will deliver an annual E-Safety CPD session for staff.
- 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
- This E-Safety policy and its updates will be presented to and discussed by staff.
- The Computing Leader will provide advice / guidance / training to individuals as required

Training – Governors:

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee involved with child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (e.g. e-PD)
• Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)

Technical – infrastructure/equipment, filtering and monitoring:

The school has a managed IT service provided by an outside contractor, that provides a content filter that is designed to prevent children from accessing adult and inappropriate content as well as preventing children from accessing extremist and terrorist material but it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

All users will have clearly defined access rights to school technical systems and devices
All users (at KS1 and above) will be provided with a username by the ICT Technician who will keep an up to date record of users and their usernames. Users at KS2 are responsible for the security of their username and password.
• The “administrator” passwords for the school IT system, used by the ICT Technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
• The Computing Leader and IT Technician are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs
• Internet access is filtered for all users by a Local Authority Approved Contractor. There is a clear process in place to deal with requests for filtering changes (see Appendix A for more details)
• An appropriate system is in place for users to report any actual potential technical incident security breach to the relevant person whilst using the school’s hardware, mobile technology or the use of the internet
• The school infrastructure and individual workstations are protected by up to date virus software
• Any temporary members of staff requiring internet access are required to sign the acceptable use form.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, 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 is 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 pupils 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 should not be used for such purposes

- Care should be taken when taking digital / video images that pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with relevant permissions from parents on the use of such images
- Pupils' 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 pupils are published on the school website to be covered as part of the agreement signed by parents or carers at the start of each academic year

Data Protection:

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

Staff must ensure that they:

- at all times, 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 personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be password protected
- the device must be password protected

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils 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 nominated person, 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.
- It is not acceptable for staff to be contacting pupils outside of school or through electronic means.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff

Social Media - Protecting Professional Identity:

Please see the staff code of conduct for reference to staff use of Social Media.

Responding to incidents of misuse:

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images there , or if there is any other suspected illegal activity e.g. grooming the Headteacher or other DMS should contact the

Children's Access Point:

Telephone: 01403 229900 Email**:** **cap@westsussex.gcsx.gov.uk**

Local Area Designated Officer (LADO)

If the matter involves an allegation against a member of staff or volunteer the

Headteacher or other DMS should contact the LADO on 0330 222 3339.

Other incidents:

It is assumed that all members of the school community will be accessing and using the school's systems appropriately. However, from time to time, children may be exposed to material that is not acceptable with in school.

When this is the case a e-safety incident form should be filled out and returned the E-Safety Lead for action.

If a member of staff believes the material has been accessed deliberately, they should fill out an E-Safety incident form along with a Red Form (please see Child Protection policy)and return both to the Headteacher.

E-Safety Incident Form – Please complete this form in the event of any concern regarding E-Safety. It should be returned either to Ross Harrison or Charlie King. In the event of a safeguarding concern, if Charlie King is not in school, return it to Kate Turner.					
Time and date:	Incident	Action taken		Incident reported by:	Signature:
		What?	By whom?		

Development/Monitoring/Review of this Policy:

- This e-safety policy has been developed by a working group made up of:
- The Senior Leadership Team
- Computing Leader
- Staff

Schedule for Monitoring Review:

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / Questionnaires of
- Pupils
- Parents / Carers
- Staff

Other Documentation to be used in conjunction with this Policy:

Plaistow and Kirdford Acceptable Use Forms (Staff and Pupils)
Child Protection Policy
Staff Code of Conduct