# DREW PRIMARY SCHOOL

## E-SAFETY POLICY

*'Learning today for tomorrow's world.'*

**Agreed at Governing Body Meeting on …………………**

**Signed Headteacher: ……………………………….………**

**Signed Chair of Governors:………………………………**

| | |
|---|---|
| Name of Policy: E-Safety policy<br>Date: 13th January 2016 | |

| | |
|---|---|
| Agreed at Policy Committee Meeting on: | 21th January 2016 |
| Signed Head teacher: | 21th January 2016 |
| Signed Chair of Governors | 21th January 2016 |

## History of Policy

| Date | Notes |
|---|---|
| January 2014 | Policy updated by COMPUTING Co-ordinator |
| January 2015 | Reviewed by Policy Committee |
| January 2016 | Reviewed by Policy Committee |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## Introduction

COMPUTING in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (COMPUTING) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies children and young people are using both *inside and outside* of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much Computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Drew Primary School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

## Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinators in our school are **Mrs E Peltier and Mr P Goodrich.** All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such Newham LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head/e-Safety coordinator updates Senior Management and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

## Writing and reviewing the e-Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, students, and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for COMPUTING, Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHE policies including Anti-bullying.

Our e-Safety policy has been written by the school, in conjunction with advice from Newham LA and government guidance. It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed regularly.

## E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

## E-Safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or on the Managed Learning Environment.
- The school website and the Managed Learning Environment contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay safe page.
- The school will send out relevant e-Safety information through newsletters, the school website, the Managed Learning Environment and the school prospectus.

### Community use of the Internet

- External organisations using the school's Computing facilities must adhere to the e-Safety policy.

## 2. Teaching and Learning

## Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety. This is clearly supported with the new curriculum and the new scheme of Rising Stars that enforces e-safety in all lessons.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

## Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## 3. Managing Internet Access

## Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School COMPUTING systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with NPW.

## E-mail

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

## Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Managed Learning Environment (MLE). This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Drew Primary School Website, particularly in association with photographs.
- Photographs of individual pupils will not be permitted to be placed on children's 'homepages'. Only Computing pictures of groups or group activities will be permitted.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

## Photographs taken by parents/carers for personal use

On the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

## Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites.

## Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- School will ensure that suitable filtering is in place. Teaching children anout online safety more generally – ( DFS – keeping children safe in education – July 2015 – pg 17)

## Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school must be switched off at the beginning of the school day and only switched off once dismissed by the class teacher.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions.

## Managing video-conferencing

- When it is introduced into our school, IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for all pupils' age.

## Protecting personal data

The school will collect personal information about you fairly and will let you know how the school and Newham LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Newham LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Newham LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Newham LA and as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

## 4. Policy Decisions

## Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school Computing resource.

## Password Security

- Adult users are provided with an individual network, email and Managed Learning Environment login username and password, which they are encouraged to change periodically.
- All pupils are provided with an individual network, email and Managed Learning Environment login username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

## Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NPW can accept liability for the material accessed, or any consequences of Internet access. The school will audit Computing provision to establish if the e-Safety policy is adequate and that its implementation is effective.

## Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

## 5. Communications Policy

## Introducing the e-Safety policy to pupils

- E-Safety rules will be displayed in all classrooms and the COMPUTING/ Computing suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.

- Pupils will be informed that network and Internet use will be monitored.

## Staff and the e-Safety policy

- All staff will be given the School e-Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

## 6. The Managed Learning Environment (MLE)

- All staff will be trained and given advice on how to effectively use the Managed Learning Environment.
- Parents will be informed about what the Managed Learning Environment is and how it can enhance the learning of each child. All children will be given training on how to effectively use the Managed Learning Environment.
- All children will be given a username and password to access secure resources and facilities through the Managed Learning Environment. Children will be allowed to choose their own password and taught to keep this secure.
- Managed Learning Environment will be regularly monitored for incidents of cyber-bullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending of messages through the Managed Learning Environment is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user of the Managed Learning Environment should such behaviour be repeated.
- Children will be allowed to upload photographs of groups or group activities onto their homepage but not individual pictures of themselves.
- Class teachers will monitor the use of the Managed Learning Environment. Any misuse of Managed Learning Environment will be reported to the Headteacher.

## 7. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness regularly. They will do this during reviews conducted between the e-Safety Coordinator, COMPUTING Coordinator, Designated Child Protection Coordinator, and Governor with responsibility for COMPUTING and Governor with responsibility for Child Protection (e-Safety committee). Ongoing incidents will be reported to the full governing body.

**Computing Concent Form:**

Parent / guardian name:

___________________________________

**Pupil name(s): __________________________ Class: ______________________**

- As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL e-mail* and other COMPUTING facilities at school.

- I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the 'rules for responsible COMPUTING use'.

- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

- I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

**Parent / guardian signature: _______________________________**

**Date: ___/___/___**

## Use of digital images - photography and video

- To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.
- We follow the following rules for any external use of digital images:
  - **If the pupil is named, we avoid using their photograph.**
  - **If their photograph is used, we avoid naming the pupil.**
- Where showcasing examples of pupils work we only use their first names, rather than their full names.
- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
- Only images of pupils in suitable uniform are used.
- Staff is not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pComputingures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

**Use of digital images - photography and video:** I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

**Parent / guardian signature: ________________________ Date: ___/___/___**

# Think before you click

**S**

I will only use the Internet and email with an adult

**A**

I will only click on icons and links when I know they are safe

**F**

I will only send friendly and polite messages

**E**

If I see something I don't like on a screen, I will always tell an adult and use Hector safety button.

My Name:

My Signature:

## KS2 Pupil Acceptable Use Agreement

*These rules will keep me safe and help me to be fair to others.*

1. I will only use the school's computers for schoolwork and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into school without permission or upload inappropriate material to my workspace.
5. I am aware that some websites and social networks have age restrComputingions and I should respect this.
6. I will not attempt to visit Internet sites that I know to be banned by the school.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
12. If I see something I don't like on a screen, I will always tell an adult and use Hector safety button.

***I have read and understand these rules and agree to them.***

*Signed:* ______________________________

*Date:* ________________________________

| Drew Primary School | |
|---|---|
| AUP review Date | March 2015 |
| Date of next Review | March 2016 |
| Who reviewed this AUP? | Paul Goodrich |

## Acceptable Use Policy (AUP): agreement form for adults working with children – in paid or voluntary capacity

Covers use of digital technologies in Drew Primary School: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the Drew Primary School digital technology resources and systems for Professional purposes or for uses deemed ‘reasonable’ by Drew Primary School.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other Drew Primary School systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the Drew Primary School data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any Drew Primary School business.
- I will only use the approved Drew Primary School email or other Drew Primary School approved communication systems with young people or parents/carers, and only communicate with them on appropriate Drew Primary School business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate contact.
- I will not download any software or resources from the Internet that can compromise my computer, or are not adequately licensed.
- I will not use personal digital cameras or camera phones for taking and transferring images of young people without permission and will not store images at home without permission.

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the Drew Primary School, is provided solely to support my professional responsibilities and that I will notify Newham of any “significant personal use” as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Drew Primary School data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to young people’s information will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the e-safety messages for adults and young people into my area of work.
- I understand that all Internet usage may be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

**User Signature**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Drew Primary School’s most recent e-safety policies.

I agree to abide by all the points above.

Signature ....................................................... Date ............................................

Full Name ..............................................................................................(printed)

Job title ........................................................................................................

Ipad Serial No: (If applicable) ……………………………………………………

Laptop Serial No: (If applicable) ……………………………………………………

.