

# **Eveline Day School E-Safety Policy**

**(With Data Protection Policy)**

**Reviewed September 2019**

## **Contents of e-Safety Policy:**

- 1. Introduction**
- 2. Context and background**
- 3. Roles and Responsibilities**
- 4. Technical and Hardware Guidance**
- 5. e-Safety for pupils**
  - a. Internet access at school
  - b. Using the Internet for learning
  - c. Teaching the safe use of the Internet
  - d. Using emails with pupils
  - e. Chat and online discussions
  - f. Other online technologies – mobile phones etc
  - g. Cyber Bullying
  - h. Contact Details and Privacy
  - i. Deliberate misuse – procedures and sanctions
  - j. Complaints
  - k. e-Safety Class Rules for KS1 and KS2
- 6. Use of Computing by school staff**
- 7. Staff Acceptable Use Agreement Form**
- 8. Data Protection Policy**

### **1. Introduction**

This policy has been discussed with staff, agreed by the senior management and approved. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world, as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

## **2. Context and Background**

### **The technologies**

Computing in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- **The Internet – World Wide Web**
- **E-mail**
- **Instant messaging (often using simple web cams) e.g. Instant Messenger)**
- **Web based voice and video calling (e.g. Skype)**
- **Online chat rooms**
- **Social networking sites (e.g. Facebook)**
- **Blogs and Micro-blogs (e.g. Twitter)**
- **Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)**
- **Video broadcasting sites (e.g. You Tube)**
- **Music and Video downloading (e.g. iTunes)**
- **Mobile phones with camera and video functionality**
- **Smart phones with e-mail, messaging and internet access**

### **Our whole school approach to the safe use of COMPUTING**

Creating a safe computing learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching embedded into the school curriculum and schemes of work

### **3. Roles and Responsibilities**

E-Safety is recognised as an essential aspect of strategic leadership in this school.

#### **Leadership team**

The SLT ensures that the policy is implemented across the school via the usual school monitoring procedures.

#### **e-Safety Co-ordinator**

Our school e-safety co-ordinator is Eveline Drut (Headteacher).

She is responsible for keeping up to date all e-Safety issues and ensuring that staff are updated as necessary.

#### **School Staff**

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed. Class teachers should ensure that pupils are aware of the e-safety rules, introducing them at the beginning of each new school year.

#### **Pupils**

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using computing at school.

#### **Parents**

The policy is available on the website and they are encouraged to support the SMART rules with their children.

### **4. Technical and hardware guidance**

#### **Downloading files and applications**

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

### **Portable storage media**

- Staff are allowed to use their own portable media storage (USB keys etc). If use of such a device results in an anti-virus message they should remove the device and immediately report to the Computing Administrator

### **Security and virus protection**

The school subscribes to the Eset internet security software. The software is monitored and updated regularly by the school technical support staff.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the Computing Administrator.

## **5. e-Safety for Pupils**

We believe it is our responsibility to prepare pupils for their lives in the modern world, and Computing is an integral part of that world. At our school we are committed to teaching pupils to use the computer effectively and appropriately in all aspects of their education.

### **Internet access at school**

#### **Use of the Internet by pupils**

Internet access is carefully controlled by teachers according to the age experience of the pupils, and the learning objectives being addressed. **Pupils are always actively supervised by an adult** when using the internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

#### **Access for all pupils**

In line with our inclusion policies across the school, we want to ensure that all pupils have access to the Internet, particularly where this will directly support their learning.

#### **Using the Internet for learning**

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and as a source of digital learning materials.

Using the Internet for learning is now part of the Computing Curriculum (Sept 2014) We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation.
- They are taught that web-based resources have similar **copyright status** as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

## Teaching safe use of the Internet and Computing

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the **Kidsmart** safety code to support our teaching in this area: **Kidsmart** has been developed by the Childnet charity, and is endorsed by the DfES <http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART tips:

- **Safe** – Staying safe involves being careful and not giving out your name, address, mobile phone no, school name or password to people online.
- **Meeting** someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present.
- **Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.  
**Remember** someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation.
- **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

## Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

## Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the

curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision and at home.

### **Unsuitable material**

Despite the best efforts of the school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experience directly to an adult at the time they occur, so that action can be taken. The action will include:

- 1 Making a note of the website and any other websites linked to it.
- 2 Informing the Computing Administrator
- 3 Logging the incident – Computing Incident Log Book in the school office
- 4 Discussion with the pupil about the incident, and how to avoid similar experiences in the future.

### **Using E-Mail at School**

E-mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- We teach the use of e-mail as part of our Computing curriculum, and use appropriate email accounts where necessary.
- Pupils are **not allowed** to access personal e-mail using school internet facilities.

### **Chat, discussion and social networking sites**

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

There is no use of chat, discussion and social networking sites in school.

### **Internet-enabled mobile phones and handheld devices**

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school,

particularly when they give access to the Internet, and allow pictures and information to be remotely posted to website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

### **Cyberbullying – online bullying and harassment**

Online bullying and harassment via instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

### **Contact details and privacy**

As specified elsewhere in this policy, pupils' personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

### **School and pupil websites – pictures and pupil input**

As part of the Computing and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

### **Deliberate misuse of the internet facilities**

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom.

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

#### **Sanctions will include:**

**Unsuitable material** (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from the class teacher
- Report to Headteacher
- Letter to parent/carer

**Offensive material** (e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to the Headteacher
- Initial letter to Parent/Carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

## **How will complaints regarding e-Safety be handled?**

It is the duty of the school to ensure that every child in our care is **safe**, and the same principles apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

International scale and linked nature of Internet content, the availability of mobile technologies and speed to change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile phone or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and Pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- All incidents will be recorded
- Interview/counselling by class teacher, Senior Management Team, e-Safety Co-ordinator and Headteacher
- Informing Parents or Carers
- Removal of Internet or computer access for a period
- Referral to Police

Our e-safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

## **9. Use of the Internet and Computing resources by school staff**

### **The Internet**

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

### **Internet Availability**

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

## **Computing Equipment and Resources**

The school also offers staff access to appropriate Computing equipment and resources, including computers, laptops, ipads, interactive whiteboards, data projectors, cameras and a range of professional and curriculum software.

## **Professional Use**

Staff are expected to model appropriate Computing and Internet use at all times, This supports our commitment to encouraging safe and appropriate Computing and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using Computers and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

## **E-mail**

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

## **Online discussion groups, bulletin boards and forums, online chat and messaging**

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

## **Social Networking**

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements.

## **Data Protection and Copyright**

The school has data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and Computing use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

## **e-Safety Policy Staff Agreement Form**

This document covers use of school digital technologies, networks etc both in school and out of school

### **Access**

- I will obtain the appropriate log on details and passwords from the Computing Co-ordinator.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
- If my password is compromised, I will ensure I change it, I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access school Computing systems or resources.

### **Appropriate Use**

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Deputy Head.
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-Safety Coordinator or member of the Senior Management Team (SMT).

## **Professional Conduct**

- I will not engage in any online activity that may compromise my professional responsibilities.
- 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 will never include pupils or former pupils as part of a non-professional social network or group.
- I will ensure that I will represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites using school facilities.
- 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 line manager / school named contact.

## **Personal Use**

- I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the following of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or social networking sites.

## **Email**

- I will only use the approved, secure email system for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents / carers, and only communicate with them on appropriate school business.

## **Teaching and Learning**

- I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet
- I will embed the school's e-Safety curriculum into my teaching, using agreed resources and materials
- I will ensure I am aware of digital safety-guarding issues to they are appropriately embedded in my classroom practice
- I will only use the Internet for professional purposes when pupils are present in a Computing suite, or a classroom with Internet access

## **Photographs and Videos**

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance)

## **Data protection**

- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media
- I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises
- I will respect the privacy of other user's data, and will never enter the file areas of other staff without their express permission

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, 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.

**Copyright**

- I will not publish or distribute work that is protected by copyright
- I will encourage pupils to reference online resources and websites when they use them in report or publication

**User Signature**

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-Safety policies.

I agree to have a school user account, be connected to the Internet via the school network and be able to use the school's Computing resources and systems.

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

Full Name.....(Printed)

Job Title.....

School.....

**Authorised Signature (Head Teacher (Primary))**

I approve this user to be set-up

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

Full Name.....(Printed)

## **9. Data Protection Policy**

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.