Colvestone Primary School

Colvestone Primary School.
E-Safety Policy.

The e-Safety Policy is important in school for a number of reasons, including:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set boundaries of use of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:
Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Office as indicated below.
The Headteacher will ensure that:
E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.

- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to *Susan Evans*

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer
    - Passwords are applied correctly to all users regardless of age
    - The IT System Administrator password is to be changed on a termly basis.

All Staff

Staff are to ensure that:
All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher /e-safety officer.
Any e-safety incident is reported to the e-Safety Officer and an e-Safety Incident report is made.

- ### All Students

- The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy
- E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school

- ### Parents and Carers

- Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletter the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

- Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded.

Technology

Colvestone School uses a range of devices including PC's, laptops, Apple Macs. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner.

Email Filtering – we use software that prevents any infected email to be sent from the school or to be received by the school.

Passwords – all staff and students will be unable to access any device without a unique username and password.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy;

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails

Photos and videos – All parents must sign a photo/video release slip when their child is admitted to the school

Social Networking –All staff must ensure their use of social media does not bring the school into disrepute, and reflects the schools standard of behaviour and staff code of conduct. See AUP.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to ICT Technicians as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME:

SIGNATURE: **DATE:**