

# **CANDARLI CUMHURIYET PRIMARY SCHOOL**

## **E-Safety Policy**

### **Introduction**

This policy has been written by school community with regarding to e-safety. It has been adapted to reflect the schools own decisions on balancing educational benefit with potential risks. This e-safety policy will be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

The school ICT coordinator and headteacher will act as E-Safety coordinators although the overall responsibility is that of the 'safeguarding persons'.

### **Rationale**

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

### **Scope**

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

### **Aims**

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning:

- Pupils will be given clear objectives for internet use.
- Only government filtered school internet is used .
- Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet:

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.

Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working:

- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely:

- Pupils will be taught about e-safety via lessons and school seminars.

Data Protection:

- There is a separate Data Protection policy.

Published content and the school web site:

- The contact details on the Web site 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:

- Photographs that include pupils will be selected carefully.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

E-mail:

- Staff will only use approved e-mail accounts when using the school network.
- Pupils are not allowed to use or make e-mail communication.
- Pupils will only use pre-defined e-mail for approved activities.

Internet Access and Learning Platform:

- Staff will read and sign the e-safety and acceptable use policies before using any school ICT resource.
- Parents will read and sign an internet access consent form and Acceptable Use Policy before their children are given access to internet resources (including the Learning Platform).
- Pupils internet access during school hours will be supervised by government filtering system. After school, parents are responsible for safety internet communication.
- All kind of social media web pages such as Facebook, Twitter, Instagram etc. are prohibited on school network.

Mobile Phones and other handheld technology:

- Pupils are not permitted to have mobile phones or other personal handheld technology in school.
- Pupils can only use smart watches if they have to communicate with their parents during school hours.

Systems Security:

- ICT systems security will be regularly reviewed with support from Schools ICT.

#### Web Filtering:

- The school will work with Schools ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to the e-safety co-ordinator.

#### Communication of the e-safety policy to pupils

Pupils will read (or be read) and sign the 'E Safety Home School Agreement' before using these resources:

- E-safety rules will be posted in each classroom where a computer is used.
- Pupils will be informed that internet and Learning Platform use will be monitored.

#### Communication of the e-safety policy to staff:

- The e-safety and acceptable use policies will be given to all new members of staff.
- The e-safety and acceptable use policies will be discussed with, and signed by, all staff.
- Staff will be informed that internet and Learning Platform use will be monitored.

#### Communication of the e-safety policy to parents/carers:

- The acceptable use policies will be available on the school website.
- Parents will be asked to sign a home-school agreement when their children join the school. This will include acceptable use policies relating to the internet, Learning Platform and other digital technologies.
- The school will communicate and publicise e-safety issues to parents through the school letters and website.

#### E-safety Complaints:

- Instances of pupil internet or Learning Platform misuse should be reported to, and will be dealt with by, the e-safety co-ordinator or headteacher.
- Instances of staff internet or Learning Platform misuse should be reported to, and will be dealt with by, the headteacher.
- Pupils and parents will be informed of the consequences of internet and/or Learning Platform misuse.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

#### Whole-School Responsibilities for Internet Safety:

##### Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to other members of Teaching Staff.
- Ensure that developments at Local Authority level are communicated to staff.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

##### Governing Body

- E-Safety will be reviewed as part of the regular review of child protection and health and safety policies.
- Support the headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the headteacher and/or designated e-safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).

### Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Embed e-safety education in curriculum delivery.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within & outside school.
- Take responsibility for their professional development in this area.

### Wider School Community:

- As a school we aim to encourage:
- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

### Parents and Carers

As a school we aim to encourage:

- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or Learning Platform.
- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

