

# E-Safety policy

Akrotiri Primary School



**Akrotiri School**

Approved by:	Ben Turner	Date: 14.11.23
Last reviewed on:	14.11.23	
Next review due by:	14.11.24	

[1 Introduction](#)

[2 Roles and responsibilities](#)

[3 Managing internet access](#)

[4 Emerging Technologies](#)

[5 Managing e-mail](#)

[6 Managing website content](#)

[7 Social networking and chat rooms](#)

[8 Mobile phones](#)

[9 Authorising internet access](#)

[10 Reporting incidents](#)

[11 Sanctions](#)

[12 Parent/carer support](#)

[13 Use of photographic images](#)

[14 Parents and friends](#)

## **1 Introduction**

1.1 This policy has been developed to ensure that all adults in Akrotiri Primary School are working together to safeguard and promote the welfare of children and young people. This policy will be ratified by the SCG annually.

1.2 E-Safety is a safeguarding issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit of using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Headteacher or, in their absence, the DSL and the SLT, have the ultimate responsibility for safeguarding (including e-safety) and promoting the welfare of pupils in their care.

1.5 This policy complements and supports Akrotiri School Safeguarding Policy and Anti-Bullying Policy. It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

## **2 Roles and responsibilities**

2.1 Both staff and pupils will be aware of the risks associated with Internet use. Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed. Staff and pupils will know what to do if they come across inappropriate material when using the Internet. Training and Inset will be provided for staff. MOD Schools support staff and teachers have put organised parents information sessions and these will be ongoing.

2.2 Internet safety depends on staff, advisors, parents, and, where appropriate, pupils themselves taking responsibility for use of the Internet and associated technologies. The school will seek to balance education with responsible use, regulation and technical solutions to ensure pupils' safety.

2.3 The use of the Internet, which brings with it the possibility of misuse will be regulated. Fair rules, written for pupils to read and understand, will be prominently displayed as a constant reminder of the expectations regarding Internet use. Teachers will visit these rules and model them within their lessons.

2.4 Effective, monitored strategies will be in place to ensure responsible and safe Internet use. The school will work in partnership with MOD Schools, parents and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

## **3 Managing internet access**

3.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people, in collaboration with the DCS IT team.

3.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

3.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

3.4 The school will work in partnership with MOD Schools to ensure systems to protect pupils and staff are reviewed and improved regularly.

3.5 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

#### **4 Emerging Technologies**

4.1 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly, in collaboration with the DCS IT team.

#### **5 Managing e-mail**

5.1 Personal e-mail or messaging between staff and pupils must not take place.

5.2 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail.

5.3 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

5.4 Access in school to external personal e-mail accounts may be used for school-related purposes only.

5.5 External incoming e-mail should be monitored and attachments should not be opened unless the author is known.

#### **6 Managing website content**

6.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

6.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

6.3 Use of site photographs will be carefully selected so that any pupils cannot be identified by name.

6.4 Learning will only be used on the website with the permission of the pupil and their parents/carers.

#### **7 Social networking and chat rooms**

7.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

7.2 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

#### **8 Mobile phones**

8.1 Children are not allowed mobile phones in school.

8.2 Mobile phones will not be used by staff to photograph children in school. The school will provide dedicated cameras or iPads.

#### **9 Authorising internet access**

9.1 All staff (including those not directly employed by the school) must read the MOD Schools Information Security Policy before using any school ICT resources.

9.2 Staff will supervise access to the internet from the School site for all pupils.

#### **10 Reporting incidents**

10.1 Staff, children and young people, parents/carers must know how and where to report incidents.

- Children – teacher.
- Staff – Technology lead / SLT
- Parents – teacher / HT / DSL

10.2 Pupils and parents/cares will be informed of the procedure for reporting incidents.

## **11 Sanctions**

11.1 Violations of the above rules will result in a temporary or permanent ban on internet use.

11.2 Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

11.3 When applicable, police or local authorities may have to be involved.

## **12 Parent/carer support**

12.1 Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website.

12.2 Parents/carers can utilise information found on Child Exploitation and Online Protection website (CEOP).

12.3 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

## **13 Use of photographic images**

13.1 Staff will be given a designated camera or iPad to use solely in school. For safe and appropriate use of photographic images we will:

- a) Ensure that all images of the pupils or staff, created or used by the school, will be used appropriately and for their intended purpose.
- b) Create and use images in order to promote or demonstrate to the school's curricular or extra-curricular provision.
- c) Primarily use images of pupils or staff in a group.
- d) Not reveal personal details such as an address or other contact details.
- e) Include images of pupils or staff on the school website that are protected so that they cannot be copied or give personal details.
- f) Allow appropriate media coverage of the school or the pupils and staff.
- g) Only share photographs with appropriate parties.
- h) Follow guidelines for GDPR.

## **14 Parents and friends**

14.1 Parents, families and friends will not create images of pupils without the knowledge of staff and pupils and that these will be used for an agreed and appropriate purpose.