AFNORTH International School - British Section

# E-Safety Policy

| | |
|---|---|
| Last Reviewed: | February 2023 |
| Next review due by: | February 2025 |

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. 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 and staff from risks and infringements.

The application of technology skills in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children. Consequently, schools need to build in the use of information technology in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology 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 ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Mobile devices
- Multimedia
- Gaming

Within the British Section of AFNORTH School, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of fixed and mobile internet technologies provided by the school.

**Roles and Responsibilities**

Responsibility

As E-Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

**The E-Safety Coordinator in our school is Peter Brown.**

Internet safety depends on all stakeholders 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 children's safety.

Effective, monitored strategies will be in place to ensure responsible and safe use of the Internet. The school will work in partnership with parents, MOD Schools, Defence Children Services (DCS) and Department for Education (DFE) to protect children.

It is the role of the E-Safety coordinator to keep abreast of current issues and guidance from DCS and through organisations such as CEOP as well as the use of online safety education programmes like 'Think U Know'. The E-Safety coordinator updates the Senior Leadership Team and School Governance Committee.

Risk Assessment

Staff and children 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 and information will be provided to parents. Children will be taught who are trusted adults, how to use technology appropriately and what to do when something makes them worried, scared or sad when using the internet

This policy, supported by the school's Acceptable Use Agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: Safeguarding, Behaviour, Health and Safety and Anti-bullying.

Regulation

The School is aware of its responsibility when monitoring the use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules, written for children 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.

- Staff and pupils are aware that MOD Schools/AFNORTH School based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the incident should be reported immediately to DCS IT department.
- If there are any issues related to viruses or anti-virus software, the DCS IT department should be informed.

**Managing School E-Safety.**

E-Safety skills development for staff.

- All members of staff receive regular information and training on E-Safety issues.
- All members of 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.
- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All members of staff incorporate E-Safety objectives, lessons and awareness within their Computing curriculum and ensure pupils apply responsible and safe Internet use in cross curricula work. E-Safety guidelines and the SMART rules will be prominently displayed around the school.

E-Safety in the Curriculum

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum. The teaching of E-Safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately. Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member.

**Managing Internet Access**

Developing good practice in internet use, as a tool for teaching and learning, is essential. School internet access will be designed expressly for staff and pupil use and will include appropriate filtering. Pupils will be taught what internet use is acceptable and given clear objectives for internet use. Staff will guide pupils in on-line activities that will support learning outcomes planned for the child's age and maturity. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. The School will work in partnership with MOD Schools to ensure systems to protect children and staff are reviewed and improved regularly. The School will take all reasonable precautions to ensure that users access only appropriate material. Neither the School nor MOD Schools can accept liability for the material accessed, or any consequences of Internet access.

Security, Data and Confidentiality

- Staff and KS2 pupils read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.
- Staff and KS2 pupils may use cloud-based storage, which is password protected to store and access information conveniently.
- Staff should be aware of their responsibilities when accessing sensitive school data:
- School data will only be accessed by staff, using their own username and password.

- School data will not be duplicated onto personally owned equipment.

School laptops and Surface Pros are encrypted and data can only be accessed using a secure log in.

**Mobile Technologies**

Managing email

The use of email within school is an essential means of communication for staff. Staff must use the AFNORTH / MOD Schools email system for any school business. KS2 children are taught about appropriate and responsible use before they are given access to an Afnorth school email address and use of Google Classroom applications.

Social Networking

The School will control access to moderated Google applications and educate children in their safe use. Children will be taught the importance of personal safety when using social networking sites and chat rooms. Should the staff be made aware of incidents or activities on these social networks which have a direct effect on the children's behaviour or attitudes within school, then the school will discuss this with parents.

Managing School Social Media and website content.

Editorial responsibility will ensure that the School's ethos is reflected in the website and on school social media platforms; 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. Photographs of children will not be used without the written consent of the children's parents. Use of photographs will be carefully selected so that children cannot be identified by name.

Taking of Images.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. The school will ensure that all images of the children or staff, created or used by the school, will be used appropriately and for their intended purpose. Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing pupil's images

All parents will be asked to give permission to use their child's photos on the school website, School social media platforms or newsletters. This consent form is considered valid for the entire period that the child attends the school unless there is a change in circumstances where consent could be an issue. Parents may withdraw permission, in writing, at any time.

### Misuse and Infringements

Complaints

Complaints or concerns relating to E-Safety should be made to the E-Safety Co-ordinator - Peter Brown or the Head Teacher.

Inappropriate use

All users are aware of the procedures for reporting accidental access to inappropriate materials or misuse

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

- Pupils – Classteacher
- Staff – the E-Safety Coordinator or the Head Teacher
- Parents – Classteacher, the E-Safety Coordinator or the Head Teacher

Inappropriate use could result in a temporary or permanent ban of School based access. Additional action may be added in line with existing practice on inappropriate language or behaviour. When applicable, police or local authorities may have to be involved.

## Parental Support.

Parents will be informed of the School's E-Safety Policy and Acceptable Use Agreement which will be accessed on the school website. Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP). A partnership approach will be encouraged with parents and this will include practical sessions as well as suggestions for safe internet use at home.