# Oakwood School
# E-Safety Policy

This policy applies to the whole school, including the EYFS

**CONTENTS:**



**Definitions:**

| | |
|---|---|
| "DfE" | Department for Education |
| "DSL" | Designated Safeguarding Lead |
| "SENCO" | Special Educational Needs Co-ordinator |

## 1 Introduction

1.1 At Oakwood, we are committed to safeguarding and promoting the welfare of all pupils in our care. Our e-safety strategy enables us to create a safe e-learning environment that:

- Promotes the teaching of Computing within the curriculum
- Protects children from harm
- Safeguards staff in their contact with pupils and their own use of the internet
- Ensures the school fulfils its duty of care to pupils
- Provides clear expectations for all on acceptable use of the internet

## 2 Roles and Responsibilities for online safety

### 2.1 Teaching e-safety

One of the key features of our e-safety strategy is teaching pupils to protect themselves and behave responsibly while online. The Head has overall responsibility for the coordination of e-safety education, but all teaching staff play a role in delivering e-safety messages in language which is appropriate to their age.

Pupils are taught:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- How adjusting their behaviour can reduce risks and build resilience, including to radicalisation
- What strategies they can use to keep themselves safe
- About the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults
- What to do if concerned about something they have seen on the internet
- Who to contact with concerns
- That the school has a 'no blame' policy so pupils are encouraged to report any e-safety incidents
- The school has a 'no tolerance' policy regarding cyberbullying
- That behaviour that breaches acceptable use will be subject to sanctions and disciplinary action

In the event that a pupil accidentally accesses inappropriate materials they must report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a pupil feels unable to disclose abuse or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk or ceop.police.uk) to make a report or seek further advice.

## 2.2 Delivering e-safety messages

- Teachers are responsible for delivering an on-going e-safety education in the classroom and will undertake regular training (normally annually) to ensure that they are up-to-date with current practice.
- Reminders are given to pupils by teachers at the start of each academic year and in specific lessons regarding the acceptable use of the internet and how to keep safe.
- Appropriate supervision is provided to ensure that pupils are accessing suitable age appropriate sites, and staff remain vigilant when computers are being used.
- Rules regarding safe internet use are clearly displayed in various relevant places.
- Pupils are expected to follow the 'Acceptable Use' guidelines outlined in Appendix A. Teachers refer pupils to these at the start of each academic year.

The following eight aspects of online education will be covered at various points in the curriculum:

Self-image and Identity; Online relationships; Online reputation; Online bullying; Managing online information; Health, wellbeing and lifestyle; Privacy and security; Copyright and ownership.

## 2.3 Evaluating and using internet content

Teachers encourage and teach good internet research skills. This includes critically evaluating retrieved information by:

- Questioning the validity of the source of information
- Comparing alternative sources of information
- Understanding the implications of copyright, correctly quoting sources and that plagiarism is against school rules

**2.4** Appropriate filters and monitoring systems are in place via the Watchguard system on the school server to safeguard children from potentially harmful and inappropriate material online, but without an unreasonable level of blocking. Wifi access points are all password protected and these are changed periodically. Guidance can be sought from the UK Safer Internet Centre by clicking here.

### 2.5 Pupils with special needs

Pupils with learning difficulties and/or any disabilities may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision. The SENCO ensures that the school's e-safety policy is adapted to suit the needs of pupils with special needs. They liaise with parents and other relevant agencies in developing e-safety practices for pupils with special needs and to keep up to date with any developments regarding emerging technologies and e-safety and how these impact on pupils with special needs.

## 3 Social Networking

### 3.1 Use of social networking sites in school

The widespread availability and use of social networking bring opportunities to understand, engage and communicate with the outside world in new ways. It is important that pupils are able to use these technologies and services effectively and flexibly. However, use of social networking applications has implications for the duty to safeguard pupils.

**3.2** Although social networking sites may be discussed in school, due to the young age of our pupils their use within school is not allowed.

**3.4** All incidents relating to e-safety and unacceptable internet use must be reported to the Head or one of the DSLs immediately.

**3.5** A log will be kept of all e-safety incidents to monitor emerging patterns of individual behaviour or weaknesses in the school's systems. These records will be kept in the central 'Incidents File'.

**3.6** If a pupil unintentionally opens a website with distressing or inappropriate content, teachers should immediately close the screen, reassure the pupil that they have done nothing wrong and report the details of the website to the Head or DSL who will then ensure that the site is blocked.

**3.7** If a pupil intentionally accesses an inappropriate website they will be subject to the sanctions set out in the Behaviour & Discipline Policy.

## 4 Cyberbullying

**4.1** Cyberbullying is the use of electronic technology, repeated over time, to intentionally hurt or upset someone. This includes devices and equipment such as computers, tablets and phones as well as communication tools including social media sites, text messages, chat and websites. The internet allows bullying to continue past school hours and invades the victim's home life and personal space and allows for hurtful comments and material to be available to a wider audience.

**4.2** Examples of cyberbullying include:

- Rude, abusive or threatening messages via e-mail, text, gaming or social networking sites.
- Posting insulting, derogatory or defamatory statements or spreading rumours on blogs or social networking sites.
- Setting up websites that specifically target a victim.
- Making or sharing derogatory or embarrassing photos or videos of someone via mobile phone or e-mail.
- Being purposely excluded from a group eg. Whats App.

**4.3** Cyberbullying can affect both pupils and staff and it could be deemed a criminal offence. Incidents of cyberbullying will be reported to the Head or Assistant/Deputy Head and if extreme may in turn be reported to the police. Pupils are taught to only give out mobile phone numbers and e-mail addresses to trusted people; not to respond to offensive messages and to report these immediately to an appropriate adult.

**4.4** Website providers and mobile phone companies are aware of the issue of cyberbullying and have their own systems in place to deal with problems, such as tracing and blocking communications and will give advice to parents and teachers on request.

## 5 Working with Parents

**5.1** Parents are expected to support the school's e-safety strategies and policies, and should talk to their children about the 'Acceptable Use' guidelines in Appendix A.

**5.2** Parents should not give their child a teacher's school email address. Any electronic communication should be made between the parent and the teacher.

**5.3** Information about e-safety will be shared with parents periodically and in a variety of different forms, eg. 'Internet Safety' booklet and 'Digital Safety' articles on the website and workshops held every few years.

**5.4** The website www.internetmatters.org helps parents to keep their children safe online. DfE advice about cyberbullying can be accessed by clicking the following link for parents.

## 6 Role of Staff

**6.1** All staff are responsible for ensuring that they use the school computers responsibly and do not personally access inappropriate content on the internet whilst at school. Detailed guidance is provided in the Staff Handbook, Code of Conduct and Acceptable Use guidelines. DfE advice about cyberbullying can be accessed by clicking the link for staff.

**6.2** The Head has ultimate responsibility for e-safety issues within the school including:

- Implementation of the school's e-safety policy
- Ensuring that e-safety issues are given high profile
- Linking with governors, parents and staff to promote e-safety
- Ensuring e-safety is embedded in the curriculum
- Ensuring that all reasonable precautions are taken to ensure that pupils cannot access inappropriate materials
- Deciding on sanctions against staff and pupils in breach of policies

**6.3** Any e-safety issues which may have serious implications for a child's safety or their wellbeing should be referred to one the DSLs without delay. Advice will be sought from the Croydon Safeguarding Children Board if escalation may be required.

## 7 Monitoring and review

**7.1** The PACT governing body supports the Head in the development and promotion of the school's e-safety strategy. The Safeguarding governor and Head monitor its effectiveness, together with the Computing co-ordinator.

**7.2** This policy will be formally reviewed every two years, however it will be amended earlier if legislation or school procedures change prior to that time.

**Signed: C Candia**

| **This policy will be reviewed every 2 years** | |
|---|---|
| Title | E-Safety |
| Version | 3 |
| Date Created | 24 May 2018 |
| Author | Ciro Candia, Head |
| Approved by SMT | Yes |
| Approval/Review required by PACT or sub-committee | No |
| Latest Review (state whether changes were made) | N/A |
| Next Review Date | Summer 2020 |

**This policy should be read in conjunction with the following related policies:**

Child Protection & Safeguarding, Behaviour & Discipline, Anti-Bullying, ICT/Computing, Staff Handbook and Code of Conduct, Acceptable Use guidelines.

Appendix A

# Acceptable Use Guidelines for Pupils

All pupils use the school's computer facilities, including internet access, as an essential part of learning. In order to ensure their safety, pupils should read the rules below and ensure they understand them. They should speak to an adult if there is anything they do not understand.

**E-safety rules for Key Stage 1:**

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do
- We can search the internet with an adult
- We always ask if we get lost on the internet

**E-safety rules for Key Stage 2:**

- We ask permission before using the internet
- We only use apps websites that an adult has chosen
- We tell an adult if we see anything we are uncomfortable with
- We immediately close any webpage we are not sure about
- We only email people an adult has approved
- We send emails and attachments that are polite and friendly
- We never give out personal information or passwords
- We never arrange to meet anyone we don't know
- We do not share passwords with other people
- We do not open emails or attachments sent by anyone we don't know
- We tell an adult immediately if we receive an offensive e-mail
- We know that bullying via e-mail or apps will not be tolerated
- We do not use internet chat rooms or access social media sites

All pupils are expected to use the school's computers, network, internet access and any other mobile devices in a responsible way at all times. They should be aware that the network and internet access may be monitored.