



**OFFORD**  
PRIMARY  
SCHOOL

# E-Safety Policy

<b>Written by:</b>	SLT
<b>Approved by:</b>	FGB
<b>Review Cycle:</b>	Annually
<b>Last review:</b>	Autumn 2018
<b>Next review:</b>	LGB Autumn 2019



## E-Safety Policy

At Offord Primary School the welfare and well-being of our pupils is paramount. The aim of this policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable user guidelines.

The purpose of this policy is to outline the safeguarding measures in place for adults and children at Offord Primary School. It explains how we aim to protect and educate pupils and staff in their use of technology and the mechanisms that exist to intervene and support any incident where appropriate. There are three main areas of risk:

1. Content: being exposed to illegal, inappropriate or harmful material;
2. Contact: being subjected to harmful online interaction with other users;
3. Conduct: personal online behaviour that increases the likelihood of, or causes harm.

The responsibility for setting and conveying these standards when using all forms of technology, is one the school shares with staff, pupils and parents. The most successful approach is one that combines site filtering, supervision, and the fostering of a responsible attitude by all and adhering to the AUP (Acceptable Use Policies) rules.

All staff and pupils are aware of all aspects of the E-Safety Policy and AUP through review and training.

### Rationale.

At Offord we believe that there are many benefits in the use of information technology, it is a constantly changing and complex information rich society that we must prepare our children to use and adapt to effectively. It is part of this which can also put our children at risk in and out of school. Some of the dangers may include:

- Exposure to inappropriate content, pornography, video games, films, substance abuse, extremist and radicalisation material/content etc;
- Lifestyle websites such as self harm, suicide and pro anorexia/bulimia;
- Hate sites and 'trolling';
- Content validation; how to check authenticity and accuracy of online content thus giving them access.

### Contact

- Grooming;
- Cyber bullying in all forms;
- Identity theft, 'frape'- hacking facebook profiles and sharing passwords.

### Conduct

- Privacy issues and not disclosing information / passwords etc;
- Digital footprint and online reputation;



- Health and wellbeing, time online;
- Sexting (personal image sharing);
- Copyright especially with music and film.

The risks are not just for children but for staff also and it is impossible to eliminate all risks completely, therefore essential through good education, to manage and minimise the risks.

#### Technology for pupils.

The school's ICT infrastructure is designed to filter inappropriate materials received into school through the E2BN, East of England Broadband Network and also through the monitoring by the Local Authorities Education ICT Service which the school buys into. If there are any materials that do seep through the schools AUP and E-Safety education programme ensure that they are equipped to deal with any issues.

#### Technologies used:

##### Staff

- Laptops/desktops/notebooks;
- Visualisers, cameras;
- Internet, E-mail, Central hosting and SIMS (Schools Information Management System), access for named staff;
- Smart boards.

##### Pupils

- Laptops/notebooks;
- Cameras;
- Visualisers;
- Internet, e-mail, data loggers, control technology equipment.

Pupils have year group and individual logins for certain programmes. All staff have individual, password protected logins to the school network and for those on supply we issue the generic password designated for them. Access can be gained via wired or wireless and the access key for wireless is securely maintained by the school office. No personal devices of staff or pupils can be connected to the schools wireless network and is not issued to any other adult or supply teacher.

#### E-Safety Curriculum

- All pupils have to sign the AUP prior to using any technologies;
- All pupils receive E-Safety training and advice through specific PSHCE related work in the Cambridgeshire programme of study;
- Assemblies and class activities throughout E-Safety week;



- Use of ThinkUKnow materials which are age related activities;
- Posters in all classrooms on SMART (Safe, Meeting, Accepting, Reliable, Tell.);
- Information issued to parents- ThinkUKnow sourced material.

### Safeguarding Children Online.

Offord Primary School recognises that different users will be expected to use the school's technology systems in different ways appropriate to age and role. We need to equip children to deal with exposure to harmful and inappropriate content, contact and equip parents to help their children feel safe when using them and also to effectively parent incidences of harmful/hurtful and inappropriate conduct by their children.

The AUP is also signed by all pupils and staff and relevant sanctions and punishments can be applied if rules are broken.

Any online misuse or problem will be reported to the Headteacher as the designated E-Safety Coordinator. A log may be kept of any incidences deemed serious.

### Responding to incidents

All members of staff must be aware of how to respond if they feel a child is at risk through their use of technology in school and or outside of school.

If a child has broken a rule on the AUP report it to the Headteacher. It is their responsibility to then:

1. Identify who is involved, any combination of child victim, child instigator, staff victim or staff instigator.
2. Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult The Child Protection Service helpline.
3. Ensure that the incident is logged on the E-Safety logging form.

Depending on the judgements made at step 1 and 2 the following actions should be taken:

Staff Instigator: Follow the policy for managing allegations made against a member of staff.

Staff Victim: Seek advice from Educational Child Protection Services or The Education Welfare Officer for Cambridgeshire

Illegal activity involving a child: Refer directly to Cambridgeshire Constabulary 0845 456 4564 making it clear it is a child protection issue.

Inappropriate activity involving a child: Follow standard child protection procedures and ensure the designated Child Protection staff are aware and involved.

Equally, if an allegation is made against a member of staff the school will follow the correct procedures for dealing with this.

Issues that come into school from home should be dealt with by the designated person and if appropriate involve the parents initially but if it involves the parents treat it as a child protection issue.

This Policy will be reviewed annually in line with child protection policies, Safeguarding and AUP.