Orchard Community Primary School

E-Safety Policy

This policy was approved by the Governing Body of Orchard Primary School at their meeting on..........................

Signed...................................... Chair of Governors

Version	Date	Author	Reason for Change
0.1	22/5/2017	AS	/
0.2	3/10/2019	JP	Updated policy to new format and removed flowcharts
0.3	6/21	FS	Added a paragraph to link with Peer to Peer abuse reference in Safeguarding Policy and wrote a section on Cyberbullying to link to the Anti-Bullying Policy

Review Frequency	Next Review Date
Every 2 years	6/2023

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

E-Safety - Roles and Responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety are the Chair of Governors, Sue Shearman (Safeguarding Link Governor), Scott Blackwell (Safeguarding Link Governor) and Mick Battle (IT Network Manager).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Deputy Headteacher/Deputy DSL/Computing Leader, John Patching, takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT Network Manager, Mick Battle, and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Network Manager

The ICT Network Manager, Mick Battle, is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

3.8 Other

The school also has a Digital Leaders committee which links to the School Council

4. Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

4.2 Curriculum Content - Implementation

- The school believes it is essential for e-safety guidance to be given to the students on a regular and meaningful basis. E-safety is embedded within the curriculum and the school continually looks for new opportunities to promote e-safety.
- The school provides opportunities within a range of curriculum areas to teach about e-safety including, but not limited to, IT and SMSC. Throughout the curriculum, students learn about internet safety and are offered advice on how to stay safe online.
- Pupils are made aware of the dangers when using the internet such as data protection, intellectual property and on-line gaming which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the ICT.

5. E-safety Skills Development for Staff/Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. They also read and sign the school's Acceptable Use Policy.

- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

- All staff are 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.
- The Deputy Headteacher/DSL/Computing Leader will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' information evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Managing the School e-safety Messages

- The School endeavours to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the beginning of each school year.
- E-safety posters will be prominently displayed in the IT suite.
- There is a dedicated e-safety page on the school website which provides information to parents and pupils, signposts for support, websites etc.

8. Incident Reporting, e-safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e-safety coordinator.

Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported to the GDPR coordinator who will report incidents to GDPR depending on the severity of the breach.

E-safety Incident Log

Minor incidents

- These could include accidental or unintentional access to unsuitable websites, Internet searches which bring up undesirable content or minor misuse IT.
- These should be recorded on the minor incident form in the IT suite and the e-safety coordinator made aware. The incidents will then be assessed in case further action is needed.

Further Action or More Serious Incidents

- Some incidents may need to be recorded on the Serious Incident Form found in the IT suite, particularly if they relate to a bullying or racist incident. Acts of Cyber Crime will be dealt with in accordance with the Computer Misuse Act 1990.
- The e-safety coordinator must be informed immediately. Further action will then be taken in accordance with CEOP and school safeguarding guidance. SMT and Head Teacher will be made aware.

Monitoring of Incidents

- All incidents will be brought to the attention of the senior management team and Curriculum Governors with information on any actions that needed to be taken and how they were resolved.

Orchard Primary School e-safety Incident Log

- Details of ALL e-safety incidents are recorded by the e-safety Coordinator. The incident logs will be monitored termly by the Head, Members of SLT Governors and the e-safety committee.

9. Misuse and Infringements

9.1 Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and the anti-bullying policy.)

9.2 Preventing and addressing cyber-bullying

E-safety practice is advocated at all times in school. At Orchard Primary School the following will take place:

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- Cyberbullying will be addressed at least termly through assemblies. It will be revisited informally through the year.
- Safer Internet Day will be used to reinforce messages regarding the safe use of technology.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Information for parents will be put on newsletters and published in the school's website; a meeting for parents to discuss internet safety will be offered annually.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- All children, parents and staff sign an Acceptable Use Agreement
- All incidents of cyberbullying must be reported to the Headteacher. This can be done directly to staff or anonymously through class worry boxes.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Whilst the school recognises that cyberbullying may take place out of school hours, it will wherever possible, step in to mediate a suitable solution.

9.3 Peer on Peer Abuse

This school recognises that children sometimes display harmful behaviour themselves and that such incidents or allegations must be referred on for appropriate support and intervention.

<u>Such abuse is unacceptable and will not be tolerated.</u>

In the context of this policy, this abuse could for example include:

- 'upskirting'
- all forms of bullying via electronic devices
- aggravated sexting

To prevent peer-on-peer abuse and address the wider societal factors that can influence behaviour, the school will educate pupils about abuse, its forms and the importance of discussing any concerns and respecting others through the curriculum, assemblies and PSHE lessons.

The school will also ensure that pupils are taught about safeguarding, <u>including online safety</u>, as part of a broad and balanced curriculum in PSHE lessons, RSE and group sessions.

All staff will be aware that pupils of any age and sex are capable of abusing their peers and will never tolerate abuse as "banter" or "part of growing up".

All staff will be aware that peer-on-peer abuse can be manifested in many ways, including sexting or cyberbullying which aims to cause emotional or psychological harm, for example.

Pupils will be made aware of how to raise concerns or make a report and how any reports will be handled – this includes the process for reporting concerns about friends or peers.

If a child has been harmed, is in immediate danger or is at risk of harm, a referral will be made to children's social care services (CSCS).

9.4 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

10. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

11. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during lessons.

Any use of mobile devices in school by pupils must be in line with the mobile phone acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

12. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Network Manager.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures, staff code of conduct or social media policy]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 2 years by the Computing Lead. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy