Orchard Community Primary School

E-Safety Policy

Version 1.0.3

Prepared By: **John Patching**

2024

Preface

This policy was approved by the Governing Body of Orchard Community Primary School at their meeting on: _ _/_ _/_2024_

Signed: ____ Chair of Governors

Version No.: **Version 1.0.3**
Created On: **02 Oct 2019**
Date of Next Review: **01 Sep 2024**

Version	Date	Author	Detail
1.0.1	**22/May/2017**	**AS**	**Issued and approved by Full Governing Body.**
1.0.2	**03/Oct/2019**	**JP**	**Updated Policy to new format and removed flowcharts**
1.0.3	**01/06/2021**	**FS**	**Added paragraph to link with Peer to Peer abuse reference in Safeguarding Policy and wrote a section on Cyberbullying to link to the Anti-Bulling Policy.**
1.0.4	**29/01/2024**	**JP**	Policy updated to align with recent KSIE regulations on student device monitoring**.**

Table of Contents

1. Aims

Our school is committed to creating a safe and positive online environment for everyone. We achieve this by:

- **Protecting:** Actively promoting and safeguarding the online safety of our pupils, staff, volunteers, and governors.
- **Educating:** Equipping all members of our school family with the knowledge and skills to navigate the digital world safely and responsibly.
- **Empowering:** Foster a culture of open communication and reporting, enabling early intervention and resolution of any online safety concerns.

2. 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 cyberbullying 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.

3. 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).

There is a governor who is responsible for and oversees E Safety

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 IT 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 (DSL)

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 Computing Leader, Network Manager and deputy DSL take 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, IT Network Manager, 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 IT Network Manager

The IT Network Manager 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 IT 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 IT 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 IT 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 IT systems and internet

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's IT 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.

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 IT.

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, ebulletins 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.
- 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

8.1 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT 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 IT 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.

8.2 E-safety Incident Log

8.2.1 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 area and the Network Manager made aware. The incidents will then be assessed in case further action is needed.

8.2.2 Further Action or More Serious Incidents

- Some incidents may need to be recorded on the Serious Incident Form found in the IT area, 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 IT Network Manager must be informed immediately. Further action will then be taken in accordance in line with school safeguarding guidance alongside the DSL team and Head Teacher.

8.2.3 Monitoring of Incidents

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

8.2.4 Orchard Primary School E-Safety Incident Log

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

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 during curriculum IT teaching and PSHE sessions and 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 signposts support to parents from the website so they are aware 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.

9.2.1 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.

Such abuse is unacceptable and will not be tolerated.

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, including online safety, 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).

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 IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Details can be found in the Acceptable Use policy.

11. Pupils Using Mobile Devices in School

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

These will be handed in at the school office and collected at the end of the day

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

To protect school data and privacy, all staff are responsible for securing their work devices when used outside school. This includes:

- **Password protection:** Keep your device password strong and unique.
- **Data encryption:** Activate data encryption to safeguard sensitive information.
- **Automatic security:** Configure screen lock and security updates automatically.
- **Responsible use:** Work devices are solely for professional work to maintain data security and protect school resources. Sharing the device with family, friends, or other unauthorized individuals is strictly prohibited.
- **Software restrictions:** Staff are encouraged to collaborate with the IT Manager for any additional software needs or inquiries. Unofficial software or applications may be removed due to potential risks to device security and school data.
- **IT support:** Should any security concerns arise, the IT Network Manager is available to offer guidance and support.

13. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT 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 IT 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 and Safeguarding Online Activity

Ensuring online safety is a top priority. Our school employs a secure monitoring system that analyses internet usage based on criteria defined by the school and our software provider. This helps us identify potential risks and keep everyone safe online.

Alerts generated by the system are carefully reviewed by the Network Manager. Any concerns are promptly escalated to the DSL team and Headteacher for a collaborative investigation.

We actively work with our internet service provider (ISP) to keep filtering procedures up-to-date. This joint effort ensures that harmful content is effectively blocked across all school devices.

Monitoring systems vary across device types. Windows and Chromebooks are comprehensively monitored through SENSO software, while iPads utilize the SENSO app when applicable based on Apple restrictions. We constantly evaluate available technologies and strive for consistent, comprehensive monitoring across all devices.

Immediate Action and Support:

- Reporting concerns: If any staff or pupil encounters inappropriate online materials, they must immediately report it to the Designated Safeguarding Lead. Investigations are initiated promptly, and any necessary device restrictions are put in place.
- Breach response: Should a breach of the Acceptable Use or Behaviour policies occur, the DSL, IT team, and Headteacher work together to address the issue and document appropriate actions.
- Supporting pupils: For pupils found accessing inappropriate materials in school, the DSL will:
  - Provide personalized support and education.
  - Offer guidance and resources to both the pupil and their parents.
  - Document the incident on the child's safeguarding record.
  - Inform parents and involve them in the support process.

15. Accounts

- Staff are provided with a local area network account with a linked email address.
- Pupils will access the local network via an individual student account.
- Staff and pupils will be provided with additional accounts as determined by the school (e.g. to access online apps and learning resources)

• Use of all school-related accounts will be in accordance with the Acceptable Use Policy.

16. E-mail

- Pupils and staff may only use approved email accounts and these will be restricted and monitored at all times.
- Email accounts of pupils may be used on infrequent occasions by teachers and pupils in their class during the teaching of using emails safely. This will be closely supervised.
- All email to school should be treated with suspicion and attachments not opened unless the author is known.

17. 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
- IT and internet acceptable use policy

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

Intentionally left blank