



**Orchard
Primary**

Online Safety Policy

Signed by:	
Head Teacher	Mrs Sarah Bitcon
Chair of Governors	Mrs S Clarke
Date of last Review	Spring Term 2026
Date of Next Review	Spring Term 2027

Contents

1. Aims	3
2. Legislation and guidance.....	3
3. Roles and responsibilities	4
4. Educating pupils about online safety.....	6
5. Educating parents/carers about online safety	7
6. Cyber-bullying.....	8
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training	11
12. Monitoring arrangements.....	11
13. Links with other policies	12
Appendix 1: KS1 acceptable use agreement (pupils and parents/carers)	
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	
Appendix 3: Acceptable use agreement (governors, volunteers and visitors)	
Appendix 4: Mobile Phone Agreement (pupils)	

1. Aims

Our school aims to:

- ✓ Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- ✓ Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- ✓ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- ✓ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- ✓ **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- ✓ **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- ✓ **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- ✓ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) 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 \(RSE\) and health 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.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Academy Standards Committee

The Academy Standards Committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Academy Standards Committee will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness.

3.2 The Head Teacher

The Head Teacher is responsible for:

- Making sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand the expectations, roles and responsibilities around filtering and monitoring.
- Making sure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Making sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.3 The Designated Safeguarding Leads (DSLs)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the Head Teacher and Academy Standards Committee to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Working with the Head Teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school Behaviour Policy.
- Liaising with other agencies and/or external services if necessary.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The ICT Manager

Through the Service Level Agreement, the ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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:

- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3) and making sure that pupils follow the school's terms on acceptable use (Appendices 1 and 2).
- Reporting any issues to the Head Teacher.
- Following the correct procedures by gaining authorisation from the Head Teacher and contacting the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS where applicable and dealt with appropriately in line with this policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify the Head Teacher/Deputy Head Teacher of any concerns or queries regarding this policy.
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)A

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

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

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).

4. Educating Pupils about Online Safety

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

All schools have to teach:

- [Relationships education and health education](#) in primary schools.

In **Key Stage One (KS1)**, 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 (KS2)** 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.
- Be discerning in evaluating digital content.

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

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- 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, 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 information and data is shared and used online.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Where and how to report concerns and get support with issues online.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents/Carers about Online Safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website.

The school will let parents/carers know what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL. Concerns or queries about this policy can be raised with the headteacher.

6. Cyber-bullying

6.1 Definition

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.

6.2 Preventing and addressing cyber-bullying

The school teaches online safety through the SCARF PSHE programme.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also provides information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected; this is available on the school website.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Head Teacher, and any member of staff authorised to do so by the Head Teacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from The Head Teacher/Deputy Head Teacher/DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

The Head Teacher/Deputy Head Teacher may examine any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Head Teacher/Deputy Head Teacher/DSL or other member of the senior leadership team to decide

on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

6.4 Artificial intelligence (AI)

Generative Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Orchard Primary School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. The use of AI will be taught within the PSHE/ICT curriculum.

Orchard Primary School will treat any use of AI to bully pupils very seriously. in line with our Anti-bullying/Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed. Staff should only use AI via the school's subscription to Teachmate AI and the Head Teacher will also use SLT AI. No other AI tools should be used.

7. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in Appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils are discouraged from bringing their mobile phones, smart watches or other electronic devices to school; however, school is aware that some parents may feel that these have a part to play in securing their child's personal safety on journeys to and from school. Pupils in Year 5 and Year 6 may therefore bring mobile devices into school, but are not permitted to use them during:

- Lessons.
- Clubs before or after school, or any other activities organised by the school.

All phones etc must be handed in to the class teacher on arrival at school. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement and Mobile Phone Agreement (see Appendices 4).

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.

9. 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.
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 3.

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 Head Teacher/Deputy Head Teacher.

10. 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 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

11.1 Staff, governors and volunteers

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.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages.
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
 - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL/Deputy DSL 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.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security

- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring Arrangements

This policy will be reviewed annually by the Head Teacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- Behaviour Policy
- Data protection policy and privacy notices
- ICT and internet acceptable use policy
- Safeguarding and Child Protection Policy



Acceptable Use of the School's ICT Facilities and Internet: Agreement for pupils and parents/carers - Key Stage 1 Pupil

Name of Pupil:

The internet and other digital information and communication technologies are powerful tools which open up new opportunities for everyone. Access to the internet is now seen as an integral part of the National Curriculum and many excellent educational resources from well-respected authorities are available on-line.

At Orchard Primary School we believe that all users should have an entitlement to safe internet access at all times. We will take every reasonable precaution, including monitoring and filtering systems, to ensure that all children will be safe when they use the internet and ICT systems.

The school will aim to ensure that all pupils have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will:

- ✓ Ask an adult for permission to use a computer/iPad.
- ✓ Only use devices or apps, sites or games which my teacher has allowed me to use.
- ✓ Not share my password with others or log in using someone else's name or password.
- ✓ Ask an adult for help if I am not sure what to do or if I think I have done something wrong.
- ✓ Tell a teacher immediately if I see anything that upsets me, or that I know is mean or wrong.
- ✓ Make sure all the messages I send are polite.
- ✓ Never give my personal information (my name, address or telephone number) to anyone online without permission from my parent/carers or teacher.
- ✓ Not open any attachments in emails, or click any links in emails, without checking with a teacher first.
- ✓ Take care of the computer and other equipment and tell a teacher straightaway if something is broken or not working properly.

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I know that if I break the rules, I might not be allowed to use a computer.

Signed (pupil):

Date:

Parent/Carer Agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/Carer):

Date:

Parent's Name (printed):



Acceptable Use of the School's ICT Facilities and Internet: Agreement for pupils and parents/carers - Key Stage 2 Pupil

Name of Pupil:

The internet and other digital information and communication technologies are powerful tools which open up new opportunities for everyone. Access to the internet is now seen as an integral part of the National Curriculum and many excellent educational resources from well-respected authorities are available on-line.

At Orchard Primary School we believe that all users should have an entitlement to safe internet access at all times. We will take every reasonable precaution, including monitoring and filtering systems, to ensure that all children will be safe when they use the internet and ICT systems.

The school will aim to ensure that all pupils have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will:

- ✓ Ask an adult for permission before I use a computer/iPad/IT equipment.
- ✓ Not share my password with others or log in using someone else's name or password.
- ✓ Only use devices or apps, sites or games which my teacher has allowed me to use and not access any inappropriate websites (inc social networking sites / chat rooms).
- ✓ Not give personal information (inc address and telephone number) to anyone or arrange to meet someone I have spoken to online.
- ✓ Ask an adult for help if I am not sure what to do or if I think I have done something wrong.
- ✓ Immediately let a teacher know if I find any material which might upset, distress, or harm me or others.
- ✓ Make sure all the messages I send are polite and responsible.
- ✓ Not take or share images of anyone without their permission.
- ✓ Not open any attachments in emails, or click any links in emails, without checking with a teacher first.
- ✓ Always use the school's ICT systems and internet responsibly and tell an adult straightaway if something is broken or not working properly.

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I know that if I break the rules, I might not be allowed to use the IT equipment.

Signed (pupil):

Date:

Parent/Carer Agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/Carer):

Date:

Parent's Name (printed):



Acceptable Use of the School's ICT Facilities and Internet: Governors, Volunteers and Visitors

You have asked to make use of our school ICT facilities. Before we can give you a log-in to our system, we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety

- I understand that the school may monitor my use of the ICT systems.
- I understand that I must use school ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will not allow unauthorised individuals to access the school network, email or internet connection.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware to the Head Teacher or a Safeguarding Lead.

I will be responsible in my communications and actions when using the school ICT systems

- I will not access, copy, remove or otherwise alter any other users' files, without their express permission.
- I will not try to upload, download or access any materials which are illegal (eg child sex abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act or which are inappropriate or may cause harm or distress to others).
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials described above.
- I understand that data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority,
- I will not use a child's full name in any email correspondence (initials only may be used).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try, unless I have permission, to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install, or attempt to install, programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understood the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further action will be taken in the event of illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community User Name	
Signed	
Date	



Use of Mobile Phones, Smart Watches and other Electrical Devices by Pupils

(Year 5 and Year 6 only)

This statement is designed to ensure that the dangers of inappropriate use of mobile phones, smart watches and other electrical devices in school are minimised and do not disrupt the pupils' education.

The increasing sophistication of mobile phone technology, smart watches and other electrical devices including the integration of cameras and accessibility to the internet, presents issues for school regarding the children's safety and wellbeing which can lead to child protection and data protection issues.

We request that parents discourage their child from bringing a mobile phone, smart watch or other electrical device to school, however we are aware that some parents may feel that they have a part to play in securing their child's personal safety on journeys to and from school.

Procedures

- If a parent feels that their child needs to bring a mobile phone, smart watch or other electrical device into school, either on a regular or occasional basis, a "Mobile Phone/Smart Watch/Other Electrical Device Agreement Form" must be completed and submitted to the Head Teacher. Only pupils whose parents have submitted this form are allowed to have a phone in school.
- Where parents give permission for their child to bring a mobile phone, smart watch or other electrical device to school they do so entirely at their own risk. The school accepts no responsibility for any loss or damage whilst the device is on school premises.
- Pupils who bring these items into school must switch it off as soon as they enter the school grounds. The device must remain switched off during the day and must not be left in pupils' bags, coats or trays.
- The mobile phone, smart watch or electrical device must be given to a member of the teaching staff upon arrival at school and signed in. It should be collected and signed for at the end of the day.
- Under no circumstances will there be access to phones during school day.
- If parents need to contact their child or pass a message to them during the school day, they should contact the School Office and not their child's mobile device.

Trips/Visits

Pupils will not be permitted to take a mobile phone, smart watch or other electrical device on school excursions.

Inappropriate Use

- If a pupil is found to have taken photographs or video footage with a mobile phone, smart watch or other electrical device of either pupils or teaching staff, this will be regarded as a

serious offence and the Head Teacher/Deputy Head Teacher will be involved from the outset. If images of other pupils or teaching staff have been taken, the device will not be returned to the pupil until the images have been deleted. The child's parent/guardian will be contacted by the Head Teacher/Deputy Head Teacher.

- In the rare circumstances that there is evidence of harassment and/or bullying the device will be confiscated and retained in a secure place by an appropriate member of staff, taking care not to delete any images or recordings which could be used as evidence.
- Parents of pupils involved in the incident will be informed without delay, unless doing so would put a pupil at risk of harm.

Sanctions

- On the first infringement, the mobile phone, smart watch or other electrical device will be confiscated by the staff member and taken to the school office. The pupil will be able to collect it at the end of the day and a record will be made of the incident. The parent/guardian will be informed of the incident.
- On the second infringement, the device will be confiscated by the staff member and taken to the school office. The parent/guardian will be notified, and the pupil will not be allowed to collect it without a parent/guardian's consent. The incident will be recorded.
- On the third infringement, the device will be confiscated by the staff member and taken to the school office. The parent/guardian will be notified, and the pupil will not be permitted to collect it without a parent/guardian being present. The school will withdraw the agreement to allow the student to bring the device to school.



Use of Mobile Phones, Smart Watches and other Electrical Devices by Pupils

Pupil Agreement			
<p>I understand that bringing a mobile phone, smart watch or other electrical device to school is a privilege that may be taken away if I abuse it. I agree to abide by the following conditions and understand the consequences if I fail to do so.</p> <ul style="list-style-type: none"> I will switch off my device as soon as I enter the school grounds and understand that it must remain switched off during the day and must not be left in my bag, coat or trays. I will immediately hand my device into the class teacher. I understand that I will not be able to access the device during school day. I will not use a mobile phone, smart watch or other electrical device to take photographs of other pupils and/or teaching staff in school. 			
Signed by Pupil		Date	

Parental Agreement			
<ul style="list-style-type: none"> I recognise that Orchard Primary School bears no responsibility for mobile phones, smart watches or other electrical devices which are lost, damaged or stolen on school property or on journeys to and from school. I will ensure that my child's device is appropriately marked so that they can recognise it. I agree to the terms of this agreement and will discuss the responsibility of owning a mobile phone, smart watch or other electrical device with my child. I understand that teaching staff may confiscate devices used in an unacceptable manner as detailed in this statement. 			
Signed by Parent		Date	
Parent's Name (print)			

Office use only:

Arbor updated		Date	
---------------	--	------	--