Online Safety Policy

Document Reference Number (if already used)	Policies/Online Safety Policy
Title	Online Safety Policy
Policy Owner	Headteacher and IT Lead
Version	1.0
Approved Date	March 2026
Approving Body	SSC
Next Review Date	March 2027

Version Control

Version	Last Modified	Last Modified By	Document Changes

Developing the roots to grow and wings to fly

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) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education - GOV.UK
- Searching, screening and confiscation

It also refers to the Department'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.

3. Roles and responsibilities

3.1 School Standards Committee

The school standards committee has overall responsibility for holding the headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on Acceptable Use of the School's ICT Systems and the internet (Appendix 1).

Members of the School Standards Committee will:

- meet with the Designated Safeguarding Lead / Online Safety Lead
- receive reports termly of online safety incidents in the Ensuring Excellence Report
- check that provision outlined in the Online Safety Policy is taking place as intended
- ensure that the filtering and monitoring provision is reviewed, at least annually.
- report to School Standards Committee

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 relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Alongside the headteacher, lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with 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 reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 IT Support

The IT support 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 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (appendix 1: Acceptable Use - Staff), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the Headteacher is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting to the IT support team using the portal **and** the School Bursar who liaises with the Internet provider.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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
- 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

Parents and carers are encouraged to support the school in reinforcing the online safety messages provided to learners in school.

Parents and carers are expected to:

- Ensure their child has read, understood (at an age-appropriate level) the terms on acceptable use of the school's ICT systems and internet (guidance on this can be found on the school website: Our School/Safeguarding/On-line Safety) and also in appendix 2: Acceptable Use – Parents & carers

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

- What are the issues? - https://saferinternet.org.uk/
- Help and advice for parents/carers - https://www.childnet.com/help-and-advice/parents-and-carers

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.

4. Educating pupils about online safety

We follow the statutory National Curriculum Programmes of Study for Computing as published by the Department for Education:

https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study

In addition, we adhere to the statutory guidance for Relationships Education, Relationships and Sex Education (RSE) and Health Education:

https://assets.publishing.service.gov.uk/media/68b96b003f3e5483efdba9b4/Relationships_Education_RSE_and_Health_Education.pdf

This will be updated in line with any revised statutory framework when implemented:

https://assets.publishing.service.gov.uk/media/6970e7e67e827090d02d42e0/Relationships_education_relationships_and_sex_education__RSE__and_health_education__for_intro_1_September_2026_.pdf

5. 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 or MyEd app. This policy will also be shared with parents and carers.

The school will let parents and carers know:

- What systems the school uses to filter and monitor online use – this information is available on our website: Our School/Safeguarding/Filtering & Monitoring
- 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 children will be interacting with online - this information is available on our website: Curriculum/Computing

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

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

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. Class teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies and online safety lessons.

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

The school also signposts information on cyber-bullying to parents and carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 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, Claude, LM Notebook and Google Gemini.

Chadsmead Primary Academy 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.

Chadsmead Primary Academy will treat any use of AI to bully pupils 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 and should carry out a risk assessment where new AI tools are being used.

6.4 Examining electronic devices

The headteacher, and any member of staff, 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 identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of 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 headteacher or Senior Leader.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Staff members may examine, and in exceptional circumstances erase, 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 headteacher or senior leader 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.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to read an agreement regarding the acceptable use of the school's ICT systems and the internet. The pupil agreements are age-phase specific. 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.

All Acceptable Use agreements are in appendixes 1 – 5.

More information on the acceptable use agreements are available on the school website: Our School/Safeguarding/Filtering & Monitoring

8. Pupils using mobile devices in school

Year 5 and 6 pupils may bring mobile devices into school, but are not permitted to use them during the school day, including before and after school clubs. Further details are available in the Mobile Phone Policy

9. Staff using work devices outside school

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

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
- 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

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Parents may be contacted.

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 code of conduct. 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.

11. 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.

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 and deputies undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors receive training on online safeguarding issues as part of their safeguarding training.

Volunteers receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The school logs behaviour and safeguarding issues related to online safety using the CPOMS system of recording.

This policy will be reviewed annually. At every review, the policy will be shared with the school standards committee.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Restorative Relationship Policy
- Child on Child Abuse Policy
- Anti -Bullying Policy
- Mobile Phone Policy
- Staff Code of Conduct Policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable Use – Staff

This will be accessed through Smart Log

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: FOR STAFF

1. Purpose

This Acceptable Use Agreement sets out the expectations for all staff who use Chadsmead Primary School's ICT systems, digital devices, network, internet access and online services. Its purpose is to promote safe, responsible, and professional use of technology in order to safeguard pupils, protect data, and support effective teaching and learning. This policy applies to all employees of the school, including permanent, temporary, and supply staff.

2. Key Principles

At Chadsmead Primary School, all staff must:

- Use technology **safely, responsibly, and professionally** at all times.
- Model positive digital behaviour for pupils.
- Protect sensitive information and follow all **Data Protection** and **Safeguarding** requirements.
- Report any concerns, incidents, or breaches promptly to the **Headteacher**, or **Designated Safeguarding Lead (DSL)**

3. Safe and Responsible Use: General Expectations. Staff must:

- Use school ICT systems and internet for **educational or professional purposes** only.
- **Keep passwords private** and never share them with others.
- **Lock or log off** devices when unattended.
- Store all files containing school or pupil data on **approved, secure platforms** (e.g. OneDrive, SharePoint).
- Report any **loss, damage, or security incident** involving school devices or data immediately.

4. Safe and Responsible Use: Communication and Conduct. Staff must:

- Communicate **professionally, respectfully, and appropriately** in all online interactions, including email and messaging platforms.
- Never use technology to **bully, harass, or embarrass** others.
- Use **school-approved channels** (e.g. official email accounts, learning platforms) when contacting pupils or parents.
- Not post images, videos, or content involving pupils or staff on **personal social media accounts**.
- Maintain the same standards of professionalism online as in person.

5. Safe and Responsible Use: Safeguarding and Child Protection. Staff must:

- Use only **age-appropriate and vetted digital content** for teaching.
- Never access, create, or share material that is **illegal, explicit, or discriminatory**.
- Immediately report any **online safety concerns** involving pupils to the **DSL** or **Deputy DSL**.
- Be alert to signs of **online bullying, grooming, or inappropriate use of technology** by pupils.
- Recognise that their behaviour online, even outside school, can impact professional reputation.

6. Safe and Responsible Use: Data Protection and Confidentiality. Staff must:

- Adhere to the school's **Data Protection and GDPR policies**.
- Access or share personal data **only when necessary** for professional duties.
- Use **school-approved devices and encrypted storage** when handling personal data.
- Ensure personal data is not stored on unapproved USB drives or personal cloud accounts.
- Dispose of personal or confidential data securely and appropriately.

7, Safe and Responsible Use: Personal Use of School ICT Systems

- Limited personal use of school ICT systems is permitted **outside teaching time**, provided it does not interfere with work duties or contravene this policy.
- Personal use must be **lawful, appropriate, and moderate**.
- The school reserves the right to **monitor usage** and restrict access where necessary.

8. Mobile Phones and Photography

- Personal mobile phones should not be used in the presence of pupils during the school day.
- Staff must **not use personal phones or cameras** to photograph or video pupils.
- All photographs and recordings of pupils must be taken using **school-owned devices** and stored securely on the school

network.

- Personal devices must **not be connected to the school Wi-Fi** unless authorised.

9. Remote Learning and Online Platforms

When conducting or supporting online learning, staff must:

- Use only **school-approved platforms** and **official school accounts**.
- Ensure their environment is **professional and private** when using video or audio communication.
- Dress appropriately and maintain high standards of conduct.
- Protect pupils' privacy and never share meeting links publicly.
- Record or capture online sessions only with **explicit permission** and for safeguarding or educational purposes.

10. Monitoring and Security

- The school's ICT systems are monitored to ensure compliance, maintain security, and safeguard users.
- Activity on school systems may be logged and reviewed in accordance with the **Data Protection Act 2018** and **school policy**.
- Any breach of this policy may result in **disciplinary action**, withdrawal of access rights, and, in serious cases, referral to external agencies.

11. Policy Compliance

By accessing the school's ICT systems, staff confirm that they:

- Have read and understood this Acceptable Use Policy.
- Will comply with its requirements at all times.
- Understand that failure to comply may result in disciplinary or legal action.

12. Declaration

I have read and understood the **Chadsmead Primary School Acceptable Use Policy for Staff**, and I agree to abide by its terms.

Appendix 2: Acceptable Use – Parents & Carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
FOR PARENTS & CARERS

Our Commitment

At Chadsmead Primary School, we believe that pupils, staff and families all share responsibility for helping children to use technology safely, respectfully and responsibly. This agreement outlines how parents and carers can support the school's approach to online safety, both at home and in partnership with us.

1. Purpose

This policy is designed to ensure that:

- Children use technology in a safe, positive and responsible way.
- Parents and carers understand how to support their child's online learning and wellbeing.
- The partnership between school and home promotes safe and responsible use of digital technologies.

2. Our Online Safety Values

We teach pupils to:

- Be kind and respectful online.
- Keep personal information private.
- Think before they post or share.
- Tell a trusted adult if something makes them worried, scared or upset.
- Use technology to learn, connect and create safely.

Parents and carers play a key role in reinforcing these messages at home.

3. Expectations for Parents and Carers

As a parent/carer of a pupil at Chadsmead Primary School, I will:

At School and in Communication with Staff

- Use the school's digital platforms (such as Arbor, or email) **appropriately and respectfully**.
- Not use social media or online platforms to **criticise or discuss** pupils, staff or the school.
- Raise any concerns through the **proper school channels** (speaking with the class teacher or Headteacher).
- Not take or share photographs or videos of pupils **during school events**, unless the school has said it is allowed.
- Respect that staff cannot respond to messages **outside of working hours** or via personal accounts.

At Home

- Support my child to **follow the school's Pupil Acceptable Use Agreement** and use devices responsibly.
- Monitor and guide my child's use of technology, including apps, websites and games.
- Encourage my child to talk to me if something online worries or upsets them.
- Set a good example by being a **positive online role model**.
- Ensure that my child's online activity **does not involve bullying, rude behaviour or sharing inappropriate material**.
- Support my child in using school devices, logins and online learning tools **only for educational purposes**.

4. Online Learning and Remote Access

If remote learning or online homework is provided, I will:

- Ensure my child uses school-approved accounts and platforms only.
- Provide a suitable space for learning where possible.
- Supervise my child's online learning and encourage **positive engagement**.
- Not share login details, meeting links or any online session recordings.
- Not record or take photos/screenshots of teachers or other pupils during online lessons.

5. Digital Images and Social Media

To help protect all members of our community, I agree to:

- Use any photos or videos of my child taken at school events **for personal use only**.
- Never post pictures of other children from school on social media without permission.
- Respect other families' and staff members' privacy online.
- Ensure that my own social media use does not bring the school into disrepute or cause upset.

6. Working Together

The school agrees to:

- Teach pupils how to use technology safely and responsibly.
- Provide clear guidance and support for parents and carers.
- Respond promptly to online safety concerns.

Parents and carers agree to:

- Support the school's approach to online safety.
- Model positive online behaviour.
- Report any concerns about online behaviour or safety to the school.

7. Agreement

I have read and understood the **Chadsmead Primary School Acceptable Use Policy for Parents and Carers**.
I agree to support the school in promoting safe and responsible technology use for all pupils.

Appendix 3: Acceptable Use – EYFS & KS1 Children

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
FOR EYFS & KS1 CHILDREN: MY ONLINE PROMISES

Our Online Safety Rules

At Chadsmead Primary School, we use computers, iPads and the internet to learn, play and create.
These promises help us to stay happy, safe and kind online.

My Online Promises

When I use computers, tablets or go on the internet at school, I promise to:

- Use kind words when I'm online or using a device.
- Listen carefully to my teacher and follow their instructions.
- Ask an adult before I go online or open a new app or website.
- Tell a grown-up straight away if I see or hear something that upsets, confuses or scares me.
- Keep my passwords and personal information private (like my full name, address or school).
- Look after the iPads, laptops and computers and use them carefully.
- Share nicely and take turns when using devices.
- Only use websites, games or apps that my teacher or trusted adult says are OK.
- Ask before taking photos or videos and never share pictures of other people without permission.
- Be a good digital citizen – using technology to learn new things, help others and make good choices.

If Something Goes Wrong

If I ever feel unsure, worried or upset about something online, I will:

- Stop what I'm doing.
- Close the laptop or put down the tablet.
- Tell a teacher, adult in school or my parents/carers straight away.

My Promise

I understand that these rules help to keep me and my friends safe when we use technology.
I will try my best to follow them every time I go online.

Name:	**Date:**

Parent/Carer Agreement

I have read and talked about these online promises with my child.
I understand that the school helps children to use technology safely and responsibly, and I agree to support this at home.

Name:	**Date:**

Appendix 4: Acceptable Use – KS2 Children

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
FOR KS2 CHILDREN: MY ONLINE AGREEMENT

Our Online Safety Rules

At Chadsmead Primary School, we use computers, iPads and the internet to learn, create and communicate. This agreement helps us to use technology safely, respectfully and responsibly.

My Online Agreement

When I use computers, tablets or the internet at school, I will:

- Use technology to help me **learn and be creative**.
- **Be kind, respectful and polite** when communicating online.
- **Listen to my teacher's instructions** and only go on websites, apps or games they have approved.
- **Keep my passwords private** and never share personal information such as my full name, address or school online.
- **Look after devices** and use them carefully.
- **Tell a trusted adult straight away** if I see, hear or read anything that makes me feel upset, worried or uncomfortable.
- **Not use technology to hurt or upset anyone**, including through messages, comments or posts.
- **Ask permission** before taking or sharing photos, videos or other people's work.
- **Think carefully before posting or sending anything online** because once it's shared, it's very hard to remove.
- **Check my privacy settings** and always act responsibly on the internet.
- **Use my time online wisely**, making sure it doesn't affect my learning or wellbeing.

If Something Goes Wrong

If something happens online that worries or confuses me, I will:

- Stop what I'm doing and turn off the screen if I need to.
- Tell my teacher, the Online Safety Lead, or another trusted adult in school.
- Talk to my parents or carers at home.
- Never try to deal with it by myself or keep it a secret.

My Promise

I understand that these rules help to keep me and others safe when using technology.
I will use computers and the internet responsibly and follow these rules both in and out of school.

Name:	**Date:**

Parent/Carer Agreement

I have read and discussed this online agreement with my child.
I understand that the school supports pupils in using technology safely and responsibly, and I agree to reinforce these messages at home.

Name:	**Date:**

Appendix 5: Acceptable Use – Visitors & Volunteers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: FOR VISITORS & VOLUNTEERS

Our Commitment
At Chadsmead Primary School, we welcome volunteers, guests and visitors who support our pupils and staff. To ensure the safety of our pupils and the security of school systems, all visitors and volunteers must follow this Acceptable Use Policy when using school ICT devices, internet, or accessing school data.

1. Purpose

This policy ensures that all visitors and volunteers understand how to use school technology responsibly, safely, and in a way that supports the school's safeguarding and professional standards.

2. General Principles

Visitors and volunteers must:

- Follow all school safeguarding and child protection policies.
- Use school technology for educational or professional purposes only.
- Respect the privacy of pupils, staff, and the wider school community.
- Report any concerns or incidents to a member of staff immediately.

3. Use of School Devices and Network

Visitors and volunteers must:

- Only use devices and accounts provided or approved by the school.
- Keep login credentials confidential and never attempt to access other users' accounts.
- Avoid installing software or connecting personal devices to the school network unless authorised.
- Use the internet responsibly and avoid visiting sites that are illegal, offensive, or inappropriate.
- Treat all devices and equipment with care and report any damage or malfunction promptly.

4. Photography and Recording

Visitors and volunteers must:

- Not take photographs, videos, or audio recordings of pupils unless given explicit permission by a member of staff.
- Respect the privacy of pupils, families, and staff when in the school setting.
- Use any approved photographs or recordings only for the purpose agreed with the school.

5. Safeguarding and Online Safety

Visitors and volunteers must:

- Maintain professional behaviour at all times.
- Not use personal mobile phones or devices in ways that could compromise pupil safety.
- Report any safeguarding concerns immediately to the Designated Safeguarding Lead (DSL) or a senior member of staff.
- Remember that any inappropriate behaviour, online or in person, may result in removal from the school site.

6. Conduct and Communication

Visitors and volunteers must:

- Communicate politely and professionally with pupils, staff, and other visitors.
- Avoid engaging in discussions online or via social media that could be seen as critical of the school, pupils, or staff.
- Follow all school instructions regarding behaviour, online use, and interactions with children.

7. Agreement

I have read and understood the **Chadsmead Primary School Acceptable Use Policy for Visitors and Volunteers**, and I agree to follow its guidelines while on school premises or using school technology.

Signed: **Date:**