

# Sparsholt C of E Primary School

## Online Safety Policy

**2025 - 2027**



|                                        |                                        |
|----------------------------------------|----------------------------------------|
| Review Frequency                       | Every 2 years (or sooner if necessary) |
| Reviewed by Safeguarding Governor      | October 2025                           |
| Next Review Date                       | October 2027                           |
| Statutory or Non-Statutory             | Non Statutory                          |
| Approved by FGB                        | 16 <sup>th</sup> October 2025          |
| Signature of Headteacher               | <i>Jane Williams</i>                   |
| Signature of Chair Full Governing Body |                                        |

## Contents

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| 1. Aims .....                                                                          | 3  |
| 2. Legislation and guidance .....                                                      | 3  |
| 3. Roles and responsibilities .....                                                    | 4  |
| 4. Educating pupils about online safety .....                                          | 6  |
| 4.1 Why is Internet use important to the school? .....                                 | 6  |
| 4.2 Pupils will be taught how to evaluate Internet content .....                       | 8  |
| 4.3 Introducing the online safety policy to pupils .....                               | 8  |
| 5. Educating parents/carers about online safety .....                                  | 8  |
| 6. Cyber-bullying .....                                                                | 8  |
| 7. Acceptable use of the internet in school .....                                      | 9  |
| 8. Managing Pupils Access .....                                                        | 9  |
| Published work and the school website .....                                            | 9  |
| Publishing pupils' images .....                                                        | 9  |
| Managing social networking .....                                                       | 10 |
| 9. Staff using work devices outside school .....                                       | 10 |
| 10. How the school will respond to issues of misuse .....                              | 11 |
| 11. Training .....                                                                     | 11 |
| 12. Monitoring arrangements .....                                                      | 12 |
| 13. Links with other policies .....                                                    | 12 |
| Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) .....    | 13 |
| Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) .....             | 15 |
| Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) ..... | 17 |

## 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
- 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.

### 3. Roles and responsibilities

#### 3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make 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.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is the **Safeguarding Governor – Eric Woodward**

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure 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

#### 3.2 The headteacher

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

The Headteacher is also responsible for:

- Ensuring an appropriate level of security protection procedures are in place, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least

annually to assess effectiveness and ensure pupils are kept 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
- Ensuring a full security check and monitoring of the school's ICT systems occur on a regular basis by liaising with the school's IT provider.
- Ensuring systems are in place to block 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.

### **3.3 The designated safeguarding lead**

Details of the school's designated safeguarding lead (DSL) and deputy (DDSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy every 2 years and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the headteacher, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers (including Governors) 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 speaking to the Headteacher or the Senior Admin Officer immediately and in their absence contacting the school's IT Provider – Drift IT
- Following the correct procedures by requesting permission from the Headteacher, who will in turn contact the school's IT provider, 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 (see appendix 5) 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.

### 3.5 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

Parents can also find multiple resources to support with Online Safety on the school's Website: [Online Safety tips](#)

### 3.6 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

### 4.1 Why is Internet use important to the school?

Internet use is a part of the statutory curriculum and a necessary tool for pupils. It is an essential tool for education, business and social interaction and the school has a duty to provide students with quality Internet access as part of their learning experience. Pupils may use the Internet widely outside school and will need to learn how to evaluate information and to take care of their own safety and security.

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
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 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 (KS) 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 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 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 be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- 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.

Developing effective practice in Internet use for teaching and learning is essential. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities.

## **4.2 Pupils will be taught how to evaluate Internet content**

Information received from the Internet require good information handling skills. In particular it may be difficult to determine origin and accuracy.

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that some pupils may, occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening; for example, to close the webpage and report the incident immediately to a teacher. The school operates a 'no-blame' policy where a pupil's first response to materials that make them feel uncomfortable is to report them to their teacher.

Pupils will be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the currency, validity and origins of information. They will learn skills to establish the author's name, date or revision and whether others link to the site. Pupils should compare web materials with other sources. Effective guided use will also reduce the chance of pupils coming across inappropriate sites.

Sparsholt C of E Primary School will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

## **4.3 Introducing the online safety policy to pupils**

- Online safety rules (created by pupils) will be posted in rooms with Internet access.
- Online safety rules will be shared with pupils on the VLE for all to access.
- Pupils will be informed that network and Internet use will be monitored.

## **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. This policy will also be shared with parents/carers.

If parents/carers 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.

## **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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### **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.

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 signposts parents and carers to information on cyber-bullying on the school's website so 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.

## **6.4 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 Bard.

Sparsholt CofE 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.

Sparsholt CofE Primary school 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.

## **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. Managing Pupils' Access**

### **Published work and the school website**

Websites can celebrate pupils' work, promote the school and publish resources for projects. The contact details on our school website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing pupils' images**

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount.

- A blanket “*Publishing Pupils’ Work and Photographs on the Website / in the Media*” letter is sent to all new pupil’s parents/carers for their written consent.
- If consent has been declined, temporary permission from parents may be sought if pupils appear in one-off group or team photographs.
- Photographs will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils’ full names will not be used anywhere on the Website or Twitter account\* particularly in association with photographs. (\* Our Twitter account is activated for the annual Year 6 residential)
- With parent’s consent, pupils’ images and videos may be shared via the school’s Yr R Tapestry portal as this can only be accessed through a valid logon. However pupils and parents are instructed not to copy these to other non-authorised social media sites.

### **Managing social networking**

Parents and teachers should be aware of social networks and other online spaces which allow individuals to publish unmediated content. Social networking sites can connect people with similar interests and guests can be invited to view content and leave comments over which there may be limited school control.

The school makes children aware of social networking; we encourage them to observe legal restrictions and educate them to make good choices:

- The school will block access to social networking sites inside school.
- Pupils are advised by the school not to join social networks until they are legally entitled to do so. Most social network sites have a 13-year age limit or older.

The school recognises its responsibility to educate pupils to make safe choices if they choose to ignore age restrictions whilst at home, and in light of this pupils are advised to:

- Never give out personal details of any kind which may identify them and / or their location.
- Recognise that any photo shared is beyond the control of the user who has shared it and may be used or adapted for purposes that the user would not wish for.
- Keep a locked down profile which doesn’t identify them as a school child.
- Recognise that social networks can never be totally safe as the user cannot manage what other members of the network do with the information shared.

### **Use of Mobile Phones**

Sparsholt CofE Primary School does not allow pupils to bring mobile devices into school from home. If a child inadvertently brings a mobile device to school, they should hand the device in at the office when they arrive at school, and pick it up at the end of the day.

## **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
- Installing anti-virus and anti-spyware software
- 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 Headteacher.

## 10. How the school will respond to issues of misuse

A minor transgression of the rules by pupils may be dealt with by the teacher / Headteacher. Other situations could potentially be serious and a range of sanctions are required. These could be linked to the **"School's Behaviour Policy"**. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct.

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

Potential child protection or illegal issues must be referred to the Designated Safeguarding Lead and Head Teacher and if necessary the Police. Advice on dealing with illegal use could be discussed with the local Police Youth Crime Reduction Officer.

- Complaints of Internet misuse by pupils will be dealt with by a senior member of staff.
- Parents / carers and pupils will need to work in partnership with staff to resolve issues.
- Sanctions may include a discussion with the Headteacher, informing parents or carers, removal of Internet or computer access for a period of time.

## 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, 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 DDSL 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.

## **12. Monitoring arrangements**

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

This policy will be reviewed at least every two years. At every review, the policy will be shared with the governing board. The review will be supported by a 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 policy should be read in conjunction with other relevant policies including

- Child protection policy
- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

## Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

### Sparsholt C of E Primary School

Woodman Lane, Sparsholt, Winchester, Hampshire, SO21 2NR

Telephone: 01962 776264

E-mail: [headteacher@sparsholt.hants.sch.uk](mailto:headteacher@sparsholt.hants.sch.uk)

[adminoffice@sparsholt.hants.sch.uk](mailto:adminoffice@sparsholt.hants.sch.uk)

[absence@sparsholt.hants.sch.uk](mailto:absence@sparsholt.hants.sch.uk)

[goinghome@sparsholt.hants.sch.uk](mailto:goinghome@sparsholt.hants.sch.uk)



Dear Parents/Carers,

### Responsible Internet Use Agreement – Reception & KS1

As part of our Computing curriculum, we are pleased to offer our pupils access to the Internet.

*Before they are allowed to use the Internet in school we would like your child to read through the Responsible Internet Use Agreement with you and for you both to sign and return the attached form to the school office.*

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide our pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The school will work with the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. To guard against access to inappropriate material we use a filtering system provided by Hampshire County Council. In addition, teachers have a duty to research and monitor areas they are intending to cover prior to use with pupils.

However unlikely, it is not impossible that children may access inappropriate material. We believe that the benefits to children from using the Internet, in the form of information resources and opportunities for collaboration, far outweigh the disadvantages.

Kind regards

School Office



## ACCEPTABLE USE OF SPARSHOLT C OF E PRIMARY SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS IN RECEPTION & KS1

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I select a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**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:**

## Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

### Sparsholt C of E Primary School

Woodman Lane, Sparsholt, Winchester, Hampshire, SO21 2NR

Telephone: 01962 776264

E-mail: [headteacher@sparsholt.hants.sch.uk](mailto:headteacher@sparsholt.hants.sch.uk)  
[adminoffice@sparsholt.hants.sch.uk](mailto:adminoffice@sparsholt.hants.sch.uk)  
[absence@sparsholt.hants.sch.uk](mailto:absence@sparsholt.hants.sch.uk)  
[goinghome@sparsholt.hants.sch.uk](mailto:goinghome@sparsholt.hants.sch.uk)



Dear Parents/Carers,

### Responsible Internet Use Agreement – KS2

As part of our Computing curriculum, we are pleased to offer our pupils access to the Internet.

*Before they are allowed to use the Internet in school we would like your child to read through the Responsible Internet Use Agreement with you and for you both to sign and return the attached form to the school office.*

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide our pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The school will work with the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. To guard against access to inappropriate material we use a filtering system provided by Hampshire County Council. In addition, teachers have a duty to research and monitor areas they are intending to cover prior to use with pupils.

However unlikely, it is not impossible that children may access inappropriate material. We believe that the benefits to children from using the Internet, in the form of information resources and opportunities for collaboration, far outweigh the disadvantages.

Kind regards

School Office



## ACCEPTABLE USE OF SPARSHOLT C OF E PRIMARY SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS IN KS2

**Name of pupil:**

*At Sparsholt School we expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere in the school. This includes the materials they choose to access and the language they use.*

**We use the computers and the Internet to help our learning. These rules will help us to be fair to others and keep everyone safe.**

- I will always ask permission before using the computers.
- I will only open, work on or delete my own files, not other pupils.
- I will not download anything without permission.
- I will not bring in USB flash drives to school.
- I will always ask a teacher before printing anything out.
- I will not change any of the computer settings.
- I will always ask permission before entering any Website unless my teacher has already approved the site
- If I accidentally find a website that I do not like or is not suitable for me, I will tell a teacher immediately.
- I will not use social media sites in school (the minimum age for using these sites is 13 years).
- I will only communicate electronically with people I know or my teacher has approved
- The messages I send will be polite and sensible.
- When sending an electronic communication to an outside agency or business I will ask my teacher to read it before I send it
- When using electronic communication, I will not give my, or anyone else's home address, phone number, other personal details or arrange to meet someone.
- I will ask permission before opening an attachment
- If I receive a message I do not like, I will tell my teacher immediately.
- I know that the school may check my computer files, read my electronic communications and monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers at school

### **Pupil's Agreement**

*I have read and understood the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times*

**Pupil's Name:**

**Class:**

**Signed (pupil):**

**Date:**

### **Parent's / Carer's Consent for Internet Access:**

*I have read and understood the school rules for Responsible Internet Use and give permission for my son/daughter/child to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of material accessed through the Internet.*

**Signed (parent/carers):**

**Date:**

**Please print name:**

### Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors)



#### ACCEPTABLE USE OF SPARSHOLT C OF E PRIMARY SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**Date:**