



# Park Gate Primary School

## Online Safety (Including Acceptable Use of ICT) Policy

### Contents

1. Aims .....	2
2. Legislation and guidance .....	2
3. Roles and responsibilities .....	2
4. Educating pupils about online safety .....	4
5. Educating parents about online safety .....	5
6. Cyber-bullying .....	5
7. Acceptable use of the internet in school .....	7
8. Pupils using mobile devices in school .....	7
9. Staff using work devices outside school .....	7
10. How the school will respond to issues of misuse .....	8
11. Training .....	8
12. Monitoring arrangements .....	9
13. Links with other policies .....	9
Appendix 1: EYFS and KS1 acceptable use agreement for pupils .....	10
Appendix 2: KS2 acceptable use agreement for pupils .....	11
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) .....	12
Appendix 4: EYFS and KS1 acceptable use agreement for parents .....	13
Appendix 5: KS2 acceptable use agreement for parents .....	14
Appendix 6: SAFE Poster Year R and KS1 .....	15
Appendix 7: SMART Poster KS2 .....	16

---

# 1. Aims

Our school aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- › Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, 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, fake news, 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 body

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, monitoring online safety as part of the monitoring of safeguarding.

All governors will:

- › Ensure that they have read and understand this policy
- › Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- › Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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.

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

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policies as well as 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
- › Working with the Deputy Head 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 child protection policy
- › Ensuring that any online safety incidents are logged using CPOMS 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 safeguarding governor.

### **3.4 The Deputy Head (in liaison Agile IT)**

The Deputy Head is responsible for ensuring:

- › An appropriate level of security protection procedures, using the filtering system FortiGuard, which is reviewed and updated on a regular basis 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
- › The school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- › Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Ensuring that any online safety incidents are logged using 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

### 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- › Working with the DSL to ensure that any online safety incidents are logged using 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'
- › Teachers are also responsible for ensuring the children understand the acceptable use agreement, getting each child to sign the class poster and displaying it in the classroom.
- › Staff are to report any suspicious activity to Agile, for the purposes of avoiding targeted phishing attacks (where fake emails are sent to capture usernames and passwords), as well as the risk of downloading and spreading ransomware.

### 3.6 Parents

Parents are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- › Read, understand and electronically agree to the terms on acceptable use of the school's ICT systems and internet (appendices 4 and 5)

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

- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet International](#)
- › Parent resource sheet – [Childnet International](#)

### 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 and Health Education](#)
- › Computing

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

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

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

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

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

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

Further details of our computing curriculum can be found in our Computing Handbook, available from our school website.

## 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. This policy will also be shared with parents.

The school will let parents know:

- › What systems the school uses to filter and monitor online use
- › 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 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Anti-Bullying 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 Development Learning, 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 sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 headteacher, and any member of staff authorised to do so by the headteacher 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, the authorised staff member will:

- › Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- › 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 cooperation

Authorised 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 headteacher 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 if 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 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 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 (electronically), 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 5). 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.

More information is set out in the acceptable use agreements in appendices 1 to 5.

## 8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices/smart watches into school, but are not permitted to use them during the school day (including before or after school clubs). All mobile phones must be turned off. Mobile phones/smart watches must be handed to the class teacher at the beginning of each day. Mobile phones/smart watches will be given back to pupils at the end of each day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which will 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
- › 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 regularly bringing the device to school and logging on

Staff members must not use the device in any way which 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 Agile IT through the Finance Officer.

## 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.

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, recordings 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 images, 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 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

Behaviour and safeguarding issues related to online safety are logged using CPOMS.

This policy will be reviewed every year by the DSL and deputy DSLs. At every review, the policy will be shared with the governing body and monitored by the Safeguarding Governor. Technology, and the risks and harms related to it, evolve and change rapidly, therefore the school will review annually new and emerging technologies and put appropriate responses in place.

## 13. Links with other policies/documents

This online safety policy is linked to our:

- Child protection and safeguarding policies
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Computing Handbook

**Policy Date: October 2023**

**Policy Review: October 2024**



## Appendix 1: EYFS and KS1 acceptable use agreement for pupils

This document will be explained to the children in school, signed by the whole class and displayed in the classroom.

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

#### **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 click on 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 I have been given
- Try my hardest to remember my username
- Keep my usernames and passwords for websites safe and not share these with others eg; TTRS
- 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.**



## Appendix 2: KS2 acceptable use agreement for pupils

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords (Years 5 and 6) safe and not share these with others
- Keep my usernames and passwords for websites safe and not share these with others eg; TTRS
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

#### **I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive or inappropriate
- Log in to the school's network using someone else's details

#### **If I bring a personal mobile phone or other personal electronic device into school (Year 6 only):**

- I will not use it during lessons, clubs or other activities organised by the school
- I will turn it off and hand it to the teacher each morning and take my phone home at the end of each day

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



## Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

### ACCEPTABLE USE OF THE 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 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:**



## Appendix 4: EYFS and KS1 acceptable use agreement for parents

This document will be sent to parents as an electronic document to read and confirm agreement.



### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

#### 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 click on 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 I have been given
- Try my hardest to remember my username
- Keep my usernames and passwords for websites safe and not share these with others eg: TTRS
- 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.**



## Appendix 5: KS2 acceptable use agreement for parents

This document will be sent to parents as an electronic document to read and confirm agreement.

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords (Years 5 and 6) safe and not share these with others
- Keep my usernames and passwords for websites safe and not share these with others eg: TTRS
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

#### I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive or inappropriate
- Log in to the school's network using someone else's details

#### If I bring a personal mobile phone or other personal electronic device into school (Year 6 only):

- I will not use it during lessons, clubs or other activities organised by the school
- I will turn it off and hand it to the teacher each morning and take my phone home at the end of each day

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

A



## Appendix 6: Online 'SAFE' Poster Displayed and Shared with Year R and KS1



The poster is titled "Internet Safety" in a large blue banner. It features a central illustration of a computer monitor, a laptop, and a smartphone surrounded by various digital icons. To the right, the acronym "SAFE" is spelled out using colorful speech bubbles, each with a corresponding instruction: "S" (green) for "SPEAK to somebody if you need help.", "A" (blue) for "ASK an adult before going online.", "F" (orange) for "FRIENDS are real people we know.", and "E" (pink) for "ENJOY Play, have fun and stay safe." Below these instructions is a group of diverse children with their arms raised in celebration. At the bottom left, a pink-bordered box contains the text "Speak to: if you are worried about anything." The footer includes the copyright notice "Copyright 2017 www.esafety-adviser.com" and the "e-safety adviser" logo.

**Internet Safety**

**S**  
**SPEAK**  
to somebody if you need help.

**A**  
**ASK**  
an adult before going online.

**F**  
**FRIENDS**  
are real people we know.

**E**  
**ENJOY**  
Play, have fun and stay safe.

**Speak to:**  
if you are worried about anything.

Copyright 2017 www.esafety-adviser.com e-safety adviser





## Appendix 7: Online 'SMART' Poster Displayed and Shared with KS2

**S**

**SHARE**  
RESPONSIBLY

We all love to share photographs, fun things we're doing and much more.

Be careful what you share and always ask permission if somebody else is in the photo or video.

**M**

**MANAGE**  
your **PRIVACY**

If you're using apps that can communicate with others, turn on privacy.

Only let people you really know follow you unless you've asked permission from your parents.

**A**

**ASK**  
for **HELP**

Don't ever be worried about asking for help from someone you trust.

You will **NOT** be judged.

**R**

**RESPECT**  
**OTHERS**

Be kind.

Other people may have different opinions from you.

That's okay, but if they become abusive, take screenshots, block and report and tell an adult.

**T**

**THINK**  
CRITICALLY

**TRUST**  
your **INSTINCT**

Is it true?  
Does that person really know me?  
Has that really happened?

Always question!

**If anything worries you,  
or if you need help with something, speak to:**

Copyright 2007  
e-safety adviser  
[www.esafety-adviser.com](http://www.esafety-adviser.com)