Eton Wick C of E First School
Policy Document

ONLINE SAFETY POLICY	
Category: Statutory	Approved by Headteacher: *Date: October 2020*
To be reviewed by: Headteacher/FGB	
To be reviewed: Annually	Overviewed by FGB: D.Stacey *Date: November 2020*
Next review due by: October 2021	

Our ethos as a church of England School is captured in the vision of good seed growing in good soil. We endeavour to provide an environment in which we are all developing, learning and growing.
Rooted in that vision, our policies have been developed.

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

⇒ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

⇒ Teaching online safety in schools

⇒ Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

⇒ [Relationships and sex education

⇒ Searching, screening and confiscation

It also refers to the 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 The governing body

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees safeguarding, including online safety is Mr Gordon Ferguson

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 1

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 DSL and deputy 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
- Working with the staff, Computing Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing body

This list is not intended to be exhaustive.

3.4 The Computing Leader

The Computing Leader is responsible for liaising with the School ICT support team to:

- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- ⇒ Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- ⇒ Conduct a full security check and monitor the school's ICT systems regularly with the schools ICT support team.
- ⇒ Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ⇒ Ensure that any online safety incidents are logged through the school safeguarding system of CPOMS and dealt with appropriately in line with this policy.
- ⇒ Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- ⇒ Maintaining an understanding of this policy
- ⇒ Implementing this policy consistently
- ⇒ Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet which is laid out in the Code of Conduct, and ensuring that pupils follow the school's terms on acceptable use appendix 1
- ⇒ Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ⇒ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- ⇒ Relationships education and health education in primary schools
- ⇒ Relationships and sex education and health education in secondary schools

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

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

The school will use assemblies and workshops to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents.

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

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

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.

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 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

⇒ Cause harm, and/or

⇒ Disrupt teaching, and/or

⇒ Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

⇒ Delete that material, or

⇒ Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

⇒ Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
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 sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

8. Pupils using mobile devices in school

Pupils should not bring a mobile phone into school. However, there may be extenuating circumstances e.g.

- Travelling to school by themselves or in a taxi.

In such cases, the mobile phone will be given to the school office as soon as they enter the building, and will collect it at the end of the day. It should not be used at any point during the school day. Further information can be found in the Mobile Phone Policy.

9. Staff using work devices outside school

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

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Computing Leader

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's 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 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 professional development meetings.

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL, along with staff, logs behaviour and safeguarding issues related to online safety. This is reported on our inline system, and is monitored weekly by the DSL

This policy will be reviewed annually by the Headteacher/DSL and Computing Leader. At every review, the policy will be shared with the governing body

13. Links with other policies

This online safety policy is linked to our:

- ⇒ Child protection and safeguarding policy
- ⇒ Behaviour policy
- ⇒ Data protection policy and privacy notices
- ⇒ Complaints procedure
- ⇒ Acceptable use policy

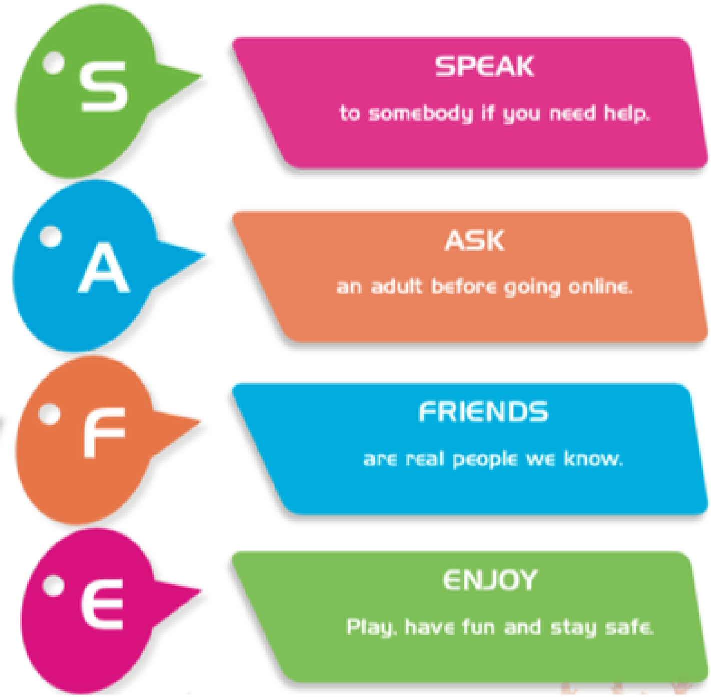
Appendix 1

Early Years and KS1 Responsible Internet Use

As many of our pupils access learning both at home and at school, it is vital a safe online environment is provided.

In school we continue to ensure the appropriate filtering and monitoring protocols are in place and any concerns relating to safeguarding of pupils including online safety, continues to be a top priority.

In KS1, we use the SAFE rules for keeping safe online. Please read and discuss these with your child. We will continue to remind the children about safe and acceptable practises online throughout the school year, and update you with relevant links.



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.

Online Code of Practice:

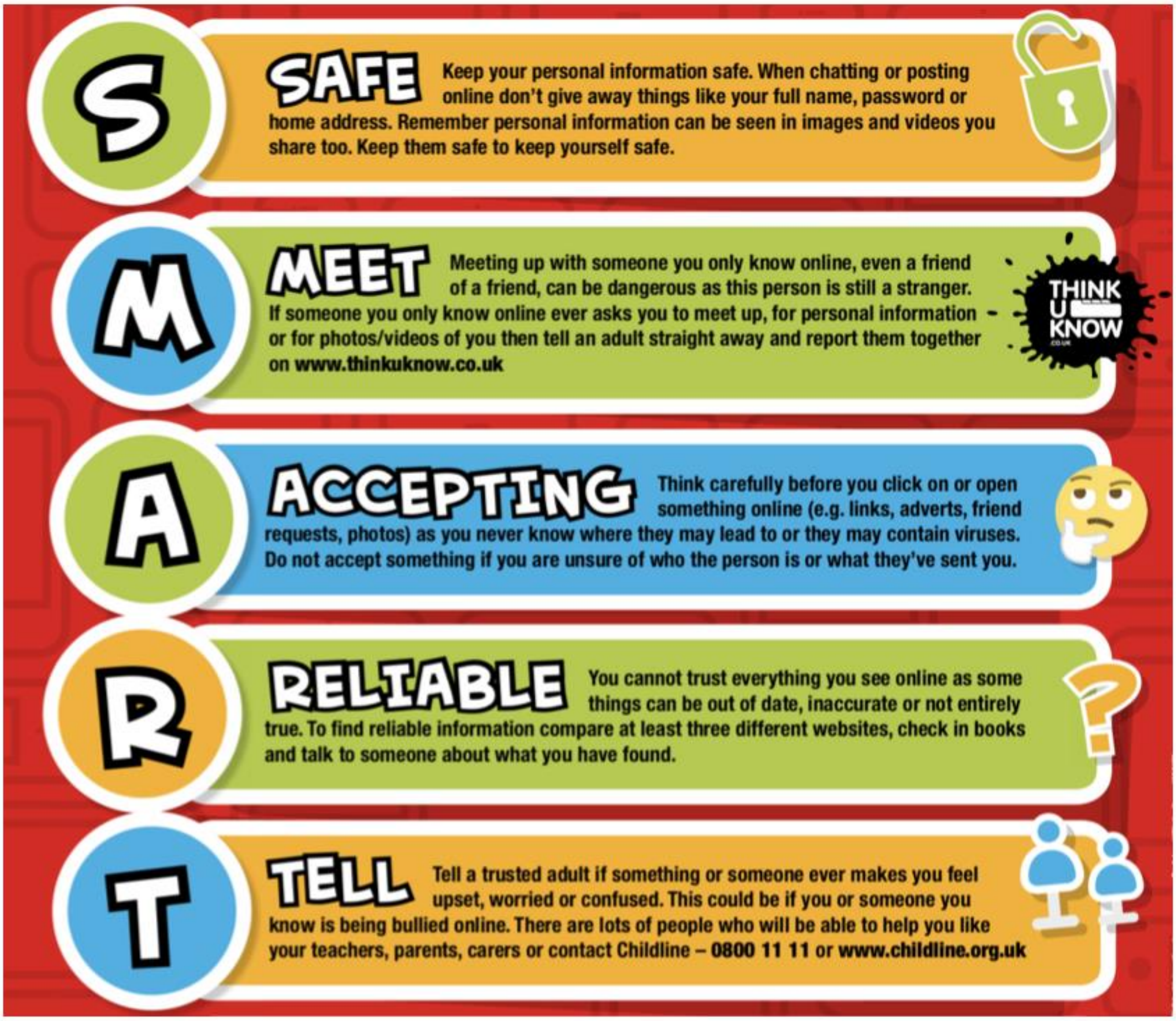
- I will only use the internet when supervised by an adult
- I will not share my passwords.
- I will make sure that messages I send are polite.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable
- I will never agree to meet a stranger
- I will keep my personal information safe (phone numbers/home and school addresses)
- I will log off when I have finished using a device
- I know that my teacher will check the sites I have visited, and my online content.

KS2 Responsible Internet Use

As many of our pupil's access learning both at home and at school, it is vital that a safe online environment is provided.

In school we continue to ensure the appropriate filtering and monitoring protocols are in place and any concerns relating to safeguarding of pupils including online safety, continues to be a top priority.

In KS2, we use the SMART rules for keeping safe online. Please read and discuss these with your child.
We will continue to remind the children about safe and acceptable practises online throughout the school year and update you with relevant links.



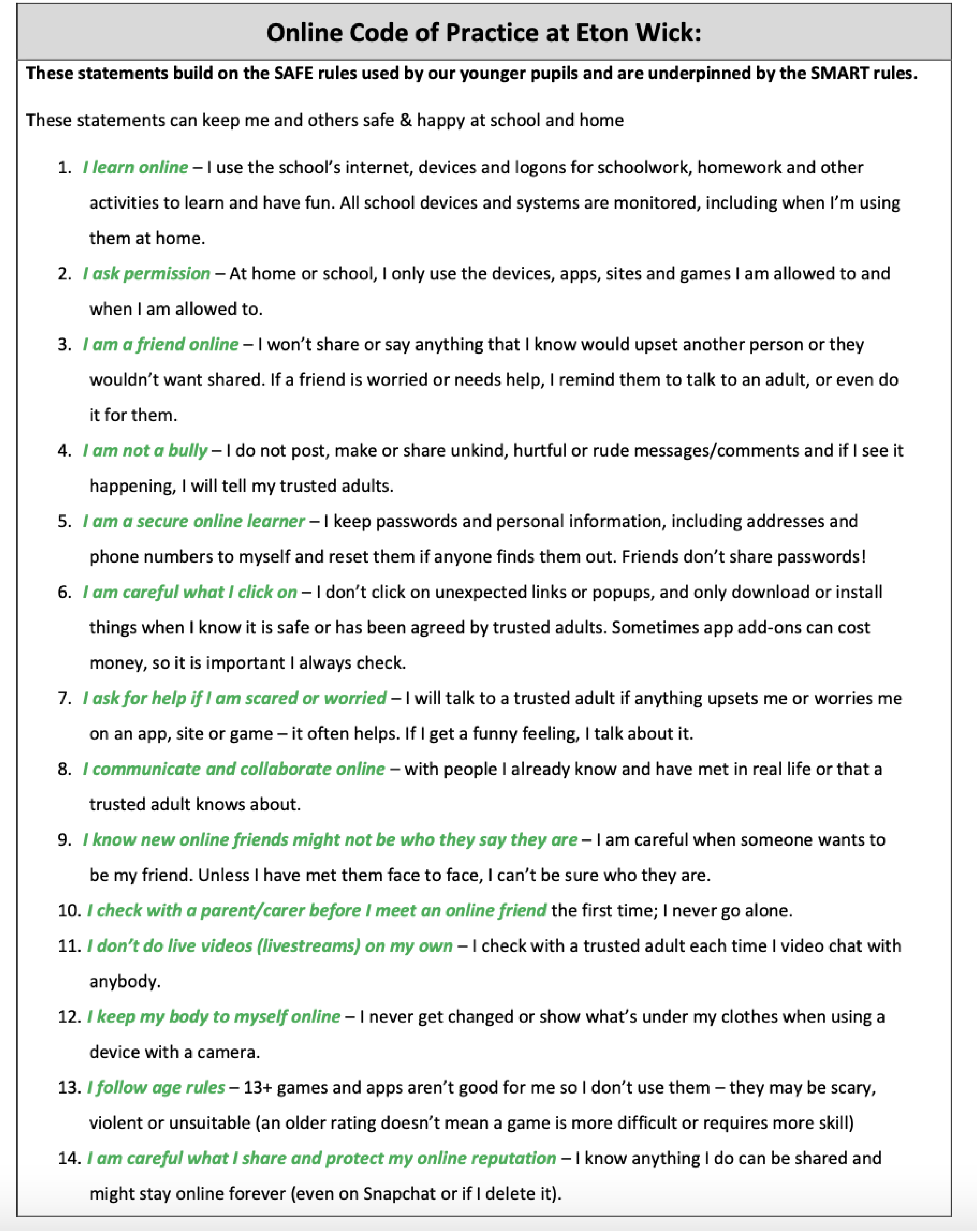
S **SAFE** Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M **MEET** Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

A **ACCEPTING** Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R **RELIABLE** You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T **TELL** Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**



Online Code of Practice at Eton Wick:

These statements build on the SAFE rules used by our younger pupils and are underpinned by the SMART rules.

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
3. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
4. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
5. ***I am a secure online learner*** – I keep passwords and personal information, including addresses and phone numbers to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
9. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
10. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
11. ***I don't do live videos (livestreams) on my own*** – I check with a trusted adult each time I video chat with anybody.
12. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera.
13. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable (an older rating doesn't mean a game is more difficult or requires more skill)
14. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).