# Online safety policy 2020-21

## St Mark’s C of E Junior School

## 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 4

6. Cyber-bullying 5

7. Acceptable use of the Internet in school 6

8. Pupils using mobile devices in school 6

9. Staff using work devices outside school 6

10. How the school will respond to issues of misuse 6

11. Training 7

12. Monitoring arrangements 7

13. Links with other policies 7

14. School ICT Agreement 8

# 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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 board

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the Internet (School ICT Agreement)

## 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.  Ensuring, where appropriate, that visitors and anyone else connected with the school, for example, contractors, agency staff and volunteers comply with this policy.

## 3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy.

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, Computing Subject 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 cyberbullying are logged and dealt with appropriately in line with the school's behaviour policy
- Updating and delivering staff training on online safety Liaising with other agencies and/or external services if necessary

### 3.4 The Computing Subject Leader

The Computing Subject Leader is responsible for the following, by overseeing the Network Manager and Technical Support (SchoolCare):

- Putting 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Coordinating and promoting the teaching of online safety through Computing, PSHE lessons and other opportunities, for example, Safer Internet Day
- Keeping up to date with online safety advice and information and working with and advising teachers, pupils, governors, headteacher, PSA and parents when needed.
- Advising on implementation of new technologies by assessing for educational benefit and safe practice.

### 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 of acceptable use of the school's ICT systems and the Internet and ensuring that pupils follow the school's terms on acceptable use
- 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's behaviour policy
- Ensuring that publication of any information online is considered from a personal and school security viewpoint.
  - no full names or any content that allows the pupils to be identified, either individually or through aggregated pieces of information.
  - photos with parental permission
  - photos where possible with individual permission
  - no names at all with photos

### 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, understood and agreed to the terms on acceptable use of the school's ICT systems and Internet

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

- What are the issues?, UK Safer Internet Centre: https://www.saferInternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- St Mark's eSafety page https://st-marks.wilts.sch.uk/esafety-2/

### 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 of acceptable use.

## 4. Educating pupils about online safety

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

Pupils will be taught to:

- Use technology safely, respectfully and responsibly, keeping personal information private and understanding ways to protect their own online identity, privacy and reputation
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact when they have concerns about content or contact on the Internet or other online technologies
- Information received via the Web, email or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. *Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.*
- Where learning how to access information is not the focus of the learning, teachers will carefully evaluate the usefulness and advantage of using online content - information should be relevant, accessible to all learners, time efficient and lead to deeper learning, eg analysis, critical thinking skills.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The use of Internet derived materials by staff and by pupils will comply with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

The safe use of social media and the Internet will also be covered in other subjects where relevant, particularly PSHE.

The school will use assemblies 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 letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings, when relevant.

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. (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. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

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 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.

Children's use of the Internet will always be supervised.  Moreover, children will be guided to specific, approved online materials and taught how to use safe search engines and techniques to keep them safe and to teach efficient learning methods.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils' email is restricted to internal email (apart from a small number of managed exceptions to allow, for example  registering for and managing approved online services) Pupil email is archived and monitored for everyone's safety.

More information is set out in the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's behaviour policy.

## 8. Pupils using mobile devices in school

Pupils may not bring mobile devices into school, including e-readers, mobile phones, iPads, iPods, digital cameras, smart watches or any device enabled to access the Internet, phone network or record media.

## 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, as set out in our School ICT Agreement.

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 Subject Leader or Network Manager.

### Staff using personal devices

Staff are provided with school equipment for the taking of photos or videos of pupils linked to an educational intention - personal devices should not be used for this purpose.
Staff may use personal devices to check email, calendar and view files.  They are to ensure that no other person, eg family member can access any school system or data, e.g. by way of shared logins or saved passwords.  No data should be stored on any personal device's hard drive.

## 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 the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

## 11. Training

All new staff members will receive training, as part of their induction, on safe Internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The 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 logs behaviour and safeguarding issues related to online safety.

## 13. Links with other policies

This online safety policy is linked to our:

- School values and ethos
- Child protection and safeguarding policy
- Behaviour policy
- Bullying policy
- PSHE policy
- Child protection policy
- Staff code of conduct for Safer Working Practice
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

# *School ICT agreement*

*The Internet and other communications technologies are powerful tools, which open up opportunities for everyone. These technologies are great for learning as they can stimulate discussion and collaboration, promote creativity and help us find information quickly. This agreement is intended to make sure that we are all aware of our responsibilities and expectations as members of this school community to keep ourselves, others and our equipment safe.  We are part of our school community at school and also at home so it is important that we apply these rules at all times and in all places. Circumstances and technologies vary and change and we must think and apply these expectations and our school values to any situation we are in.*

## *School responsibilities and expectations*

- *The school will try its best to ensure that you have good access to ICT to enhance your learning.*
- *School will monitor your use of ICT.*
- *School will take action if you are involved in incidents that break this agreement.*

## *All users of the school systems  (Staff, Governor, Visitor and Pupil) responsibilities and expectations*

- *I will treat my username and password like my toothbrush - I will not share it or use anyone else's!  I will always log out or lock when I leave a computer. I will use suitably complex passwords and change them if I think they may be known to anyone else.*
- *I am aware that the Internet is an amazing resource, but also contains information that is: inaccurate, harmful, illegal, commercial and inappropriate and so I will be careful to avoid such content.*
- *I will always be polite and respectful with others online.*
- *I will make sure people are happy before I take and/or use photos and videos of them.*
- *I will only use the photos and videos I've taken with permission and will not name children in my photos or give any information so they can be identified.*
- *I will keep school data on school devices and system, not saving to personal devices or systems.*
- *I will respect other people's work on the Internet and not copy it without saying where it came from.  I will ensure that I have permission to use the original work of others in my own work.*
- *Where work is protected by copyright, I will not download or distribute copies (including music and videos).*
- *I will prevent viruses spreading by only opening emails and attachments from people I trust and using j2e/Google Apps/365 to transfer work from home rather than memory sticks.*
- *I will immediately report any illegal, inappropriate or harmful material or incident.*
- *I will treat school equipment with great care and as directed.*
- *I will immediately report any damage or faults involving equipment or software, however this may have happened.*

## *Pupil - responsibilities and expectations*

*In addition to responsibilities and expectations for all users (see above):*

- *I will only use computers and devices when I have permission and am supervised.*
- *At home, I will follow family agreements about using computers and devices.*
- *I will agree with my parents a balance of using technology and other activities, bearing in mind the health risks of too much screen time.*
- *I will be aware of stranger-danger when communicating online, for example, I will not share personal information like my surname or a named photograph, address, telephone number, email, school etc or arrange to meet with anyone.*
- *I will immediately report to an adult anything unpleasant or that I know is inappropriate or makes me feel uncomfortable.*
- *I will use sensible names for documents and save regularly to protect my work.*
- *I will try to use websites that my parents/teachers know about and are happy with.*
- *I understand that the purpose of Computing in school is to support my learning and that's what I will use it for.*
- *I will not use any personal device in school to take photos or record media.*

## *School staff, governors and visitors - responsibilities and expectations*

***In addition to responsibilities for all users (see overleaf):***

- *I will demonstrate high standards and examples in all expectations and responsibilities.*
- *I will embed online safety ideas and skills in my practice and teaching.*
- *I will always supervise and guide children in their use of the Internet.*
- *I will communicate with pupils and parents through official school systems.*
- *I will ensure that any activity in or out of school does nothing to damage the reputation of the school or profession, e.g. content/comments on social media.*
- *I will be systematic in my storage of documents, save regularly and back up my files to protect my work.*
- *I will not take or store photos or videos of children on any personal devices or systems.*
- *I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential (except when required by law or by school policy to disclose such information to an appropriate authority).*
- *I will take care not to overload the school system or equipment with large quantities of files, eg outdated or duplicated files. I will be organised in storing data and regularly check, tidy and delete unneeded files, eg photos and videos.*

## *Parents - responsibilities and expectations*

*We appreciate that parents and carers have a crucial role and responsibility to teach children about online safety and behaviour.*

- *I will follow our school policy on the use of photos/videos – not sharing photos online that identify children in any way. Not all parents are happy to share children's photos online. We respect those wishes (which are sometimes for child protection reasons).*
- *I will be careful not to identify children by referring to them by name when commenting on blogs online.*
- *I have read through this agreement with my child and reinforced the importance of online safety at school and home.*
- *We have a family agreement for when and where my child can use the Internet. I will ensure they have a balance of technology and other activities, e.g. physical/social activities. I will bear in mind the health risks related to too much screen time, e.g. near to bed time.*
- *I will talk to my child about their use of technology and show an interest in what they are doing.*
- *I will set a good example to my children by using social media e.g. Facebook in a positive, responsible way.*
- *I will keep myself informed of online safety topics, for example by reading the Vodafone Digital Parenting magazine or visiting links on the Internet eg [www.internetmatters.org](http://www.internetmatters.org) (There are lots of other links on the school website)*
- *I am aware of the dangers of using computers and the Internet and understand how to take precautions to protect my child at home, for example using children logins, filtering and monitoring, supervised use and family agreements.*
- *I will not send children to school with devices that are enabled to access the phone network or take photos or media, eg smart watches.*

***Name(s) (Printed)*** ________________________________

***Signed:***__________________________________________

***Date:***____________________________________________

Please tick:

□ Pupil
□ Parent
□ School staff
□ Governor
□ Visitor