# Online Safety Policy

| | | | |
|---|---|---|---|
| Last Review: | **February 2024** | | |
| Approved by: | Governing Body | Date: | 30th March 2024 |
| Next Review Date: | **February 2025** | | |

# Contents

# 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 2022, and its advice for schools on:

- Teaching online safety in schools 2023
- 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.

Our school employs EGG (www.softegg.co.uk) to monitor data coming into our school server from outside sources (internet) and data inputted and communicated

outside the school server environment. When a possible infraction of our 'Online Safety Policy' is flagged, the School Business Manager will receive an email with the relevant information. This will be copied into an online safety log (Appendix 4).The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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)

## 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 DDSLs 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, School Business Manager, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring 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 logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- 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

This list is not intended to be exhaustive.

## 3.4 The School Business Manager

The School Business Manager is responsible for:

Ensuring external companies are:

- 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
- Conducting a full security check and monitoring the school's ICT systems on a regular 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 (see appendix 4) 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 (see appendix 4) 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, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody  Online grooming - Our story | Breck Foundation

## 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:

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
- Acceptable, safe and age appropriate use of social media/networks
- Identify a range of ways to report concerns about content and contact

- To realise that information inputted at school is recorded by the ISP (Internet Service Provider), EGG and the St Clement's School.
- 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. Control of data is often lost when put online or using a digital device. Some websites will claim copyright of individual data and media.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- There can be legal consequences of online actions.

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

## 5. Educating parents about online safety

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

Online safety will also be covered during 'Meet the Teacher' meetings in the Autumn term. 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 (appendices 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## 8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Smart Watches are not allowed in class. There is an exemption for basic Fitbits that do not have messaging capabilities.

## 9. Staff using work devices inside/outside of 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 – always install the latest updates
- Contact with pupils should only be made via the use of school email accounts, Google Classroom or telephone equipment when appropriate. Other online programs (TinkerCAD, scratch) may be used to contact children if it is required to fulfill curriculum requirements in computing. The St Clement's email address should be used in this instance and a member of the Safeguarding team should be notified.

- Staff should exercise caution in their use of all social media or any other web based presence that they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others.

- 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 the School Business Manager.

## 10. Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At St. Clement's no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded about the importance of not sharing without permission.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images that could reveal the identity of others and their location. We teach them

about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

## 11. Social media: St. Clements SM presence

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. A designated member of staff responsible for managing/ uploading to our Twitter account with Computing lead monitoring it overall. Only children who have received consent will feature on our Twitter.

## 12. 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.

## 13. 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 and DDSLs 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.

## 14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the computing and online safety lead. At every review, the policy will be shared with the governing board.

## 15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

# Appendix 1: Acceptable use agreement (pupils and parents/carers)

**Safe Use Agreement for Parents/Guardians for Internet Use**

Dear Parents,

As part of the new National Curriculum and the development of computing skills, e-safety is an imperative part to our children's learning, understanding and well-being within both computing lessons and in their daily lives.

Please would you read the attached *Rules for using the Internet Safely* that children need to sign, then sign and return the attached consent form.

In school, we take positive steps to dealing with any e-safety concerns, including making children aware of the e-safety rules and how to keep themselves safe during computing and PSHE lessons as well operating filtering system that restricts access to inappropriate material. Furthermore, websites that are deemed inappropriate are blocked. In rare instances, the filtering may not work. When this happens EGG will be contacted by a member of staff and the inappropriate content will be blocked.

This may not however be the case at home and we would strongly recommend for you to monitor your child's Internet use and apply parental controls where available. Please contact us if you require assistance with this.

Parents should be aware that the following online social media/networks such as: Google Classroom, TinkerCAD and Scratch are used as part of the computing curriculum.

- We suggest you consider the following:
- Keeping the computer / laptop / tablet / phone to which children are accessing the Internet in a communal area of the home;
- Ask your children how the computer and Internet work;
- Monitor on-line time and be aware of excessive hours spent on the Internet;
- Take an interest in what your children are doing by discussing with them what they are seeing and using on the Internet, including what is inappropriate material and how they should respond to unsuitable material or requests;
- Be mindful that although a lot of social networking sites are aimed at adults and adolescents over the age of 13, some children below this age have accounts and are regularly using them. This may lead to accessing

inappropriate material or behaviour and occasionally, bullying. If such matters arise, it is not the school's responsibility to deal with them.

- Be aware that children may be using the Internet in places other than in the home or at school;
- Be aware of the safety issues of mobile phones as well as game consoles that have access to the Internet. If supplying a mobile for your child, if they are walking to and from school by themselves (Year 6 only), we advise that you choose one that has no Internet access or where access can be restricted. Please note that if children consistently use their phones inappropriately, i.e. by accessing the Internet or such like, the privilege to bring a phone onto the school premises will be revoked. During school time, all mobiles should be handed to their class teacher, which are then kept in the office.
- Be aware that data shared online can be accessible by your ISP.

There are many websites now available which help you to understand more about e-safety at home:

- **CEOP Think You Know** - https://www.thinkuknow.co.uk/parents
- **Childnet International** - http://www.childnet.com/parents-and-carers
- **Hertfordshire Grid for Learning** - http://www.thegrid.org.uk/eservices/safety/parents.shtml
- **UK Safer Internet Centre** - http://www.saferinternet.org.uk/advice-and-resources/parents-andcarers/parental-controls
- Home - Safer Internet Day
- Online grooming - Our story | Breck Foundation

For further information, please see our Online Safety Policy, which is available on our website.

---

Safe Use Agreement for Parents/Guardians for Internet Use

Pupil Name(s): _____ Class(es): _____

As the parent or legal guardian of the above pupil(s), I give my permission for my son or daughter to have access to the Internet in school.

I have read both the Rules for using the Internet safely and the Safe Use Agreement for Parents/Guardians for Internet Use from the school's E Safety policy and I support my child and the school in developing safe and responsible use of the Internet.

Parent/Guardian Signature: _____

Date: _____

## Appendix 2: Children's rules for using the internet (staff, governors, volunteers and visitor

# Rules for using the Internet Safely

I will:

- Ask permission from a member of staff before using the

Internet;

- Only visit websites suitable for children my age;
- Be polite and show respect when communicating with others;
- Keep my personal information private (including name, address, telephone numbers and passwords);
- Never agree to meet someone I have met on the Internet;
- Report any unpleasant messages/inappropriate websites to a member of staff.

My Name: _____

My Signature: _____

Date: _____

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

**Code of Conduct of ICT**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without permission from the head teacher.
- I understand that my use of school information systems, Internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised manager.
- I will not install software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-safety Lead, the designated child protection officer or head teacher.
- I will ensure that electronic communications with children including e-mail, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I understand that contact with pupils should only be made via Google Classroom. Other online programs (TinkerCAD, scratch) may be used to contact children if it is required to fulfil curriculum requirements in computing. The St Clement's email address should be used in this instance and a member of the Safeguarding team will be notified.

- I will exercise caution in my use of all social media or any other web based presence that I have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others.

- I will promote e-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's ICT systems to intercept e-mail and delete inappropriate materials where it believes unauthorised use of the schools information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Name: ……

Signed: ……

Date: ……

Headteacher: ……

Date: ……