

**ONLINE SAFETY POLICY – September 2020**

# **Rationale**

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote child achievement, to support the professional work of staff and to enhance the school’s management, information and business administration system. Benefits include:

* Access to worldwide resources and research materials at the touch of a button
* Educational and cultural exchanges between children worldwide
* Access to experts in many fields
* Staff professional development such as access to online learning and forums
* Communication with support services, professional associations and colleagues
* Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The statutory computing curriculum requires children to learn how to locate, retrieve and exchange information using digital technologies. Consequently, in delivering the curriculum, teachers need to plan to integrate the use of digital technologies and web-based resources including e-mail (or e-mail simulators) to enrich learning activities. Effective internet use is an essential life skill.

# **1. Aims**

Access to the school's network and use of digital facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy.

The Aims of this Acceptable Use Policy are to: -

* + Allow all users access to school digital resources and use of the Internet for educational purposes.
  + Provide a mechanism by which staff and children are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
  + Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
  + Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
  + Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

# **2. Legislation and guidance**

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on:

* [Teaching online safety in schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)
* [Preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [cyber-bullying: advice for headteachers and school staff](https://www.gov.uk/government/publications/preventing-and-tackling-bullying)
* [[Relationships and sex education](https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education)
* [Searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation)

It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

# **3. Roles and responsibilities**

**3.1 The governing board**

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

The governing board will 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 online safety is Julie Holmes(Safeguarding and child protection governor).

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 Executive Headteacher**

The Executive 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 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:

* 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 lead and other staff, as necessary, to address any online safety issues or incidents
* 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 logged and dealt with appropriately in line with the school behaviour policy
* Updating and delivering staff training on online safety (appendix 3 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 Computing subject lead**

The Computing subject lead is responsible for line managing and instruction of the external ICT technician for:

* 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 fortnightly 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

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 (appendix 2), 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 (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
* Using the schools wi-fi code within school to connect to the internet. 4G or other providers must not be used.

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 (appendix 1)

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](https://www.childnet.com/resources/parents-and-carers-resource-sheet)

**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 2) The schools wifi-code must always be used at school to connect to the internet. 4G or other providers must not be used.

# **4. Educating pupils about online safety**

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

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

* [Relationships education and health education](https://schoolleaders.thekeysupport.com/uid/8b76f587-7bf6-4994-abf0-43850c6e8d73/) in primary schools

This new requirement includes aspects about online safety.

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
* How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

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 school 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. (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](https://www.gov.uk/government/publications/searching-screening-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, 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 and 2). 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 and 2.

# **8. Pupils using mobile devices in school**

Pupils 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 appendix 1). All mobile phones **must be switched off** and then handed to the class teacher on entry to the school and stored in an appropriate place until the end of the day.

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.

# **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 appendix 2.

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. The Music Federation actively encourage the use of Google Drive for sharing resources.

If staff have any concerns over the security of their device, they must seek advice from the Computing lead, business manager or technician.

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 Behaviour and Computing policies. 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, 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. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the Computing subject lead. At every review, the policy will be approved and ratified at a full governing body meeting.

# **13. 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
* Computing (this includes internet acceptable use)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | |
|  |  | |

# **Appendix 1: KS2 acceptable use agreement (pupils)**

|  |  |
| --- | --- |
| ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
| **Name of pupil:** | |
| **I will read and follow the rules in the acceptable use agreement policy**  **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 school related purposes only. * Only use them when a teacher is present, or with a teacher’s permission. * Keep my username and passwords safe and not share these with others. * 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’m 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. * Log in to the school’s network using someone else’s details. * Arrange to meet anyone offline without first asking my parent/carer, or without adult supervision.   **If I bring a personal mobile phone or other personal electronic device into school:**   * I will not use it during lessons, clubs or other activities organised by the school, without a teacher’s permission. * I will switch off my mobile phone as I enter the school building and hand it to the teacher at the start of the school day and will be given it back at the end of the day. * I will not turn it on until I leave the school building.   **I agree that the school will monitor the websites I visit and I understand that breaking these rules may result in a ban from using the computers/ internet or behaviour related sanctions being applied if I don’t follow the rules.** | |
| **Signed (pupil):** | **Date:** |

# **Appendix 2: 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 will use the schools wifi code to connect to the internet and will NOT use 4G or other providers.  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 computing subject lead 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 3: online safety training needs – self audit for staff**

|  |  |
| --- | --- |
| ONLINE SAFETY TRAINING NEEDS AUDIT | |
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? |  |
| Do you know what you must do if a pupil approaches you with a concern or issue? |  |
| Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors? |  |
| Are you familiar with the school’s acceptable use agreement for pupils and parents? |  |
| Do you regularly change your password for accessing the school’s ICT systems? |  |
| Are you familiar with the school’s approach to tackling cyber-bullying? |  |
| Are there any areas of online safety in which you would like training/further training? |  |

# **Appendix 4: Online safety incident report log**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ONLINE SAFETY INCIDENT LOG | | | | |
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |