

# The Richmond School, Skegness

## eSafety Policy

**Approved by:**

**Date:**

**Last reviewed on:**

January 2020

**Next review due by:**

January 2022

# 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 .....	4
7. Acceptable use of internet-enabled devices in school .....	5
8. Pupils using mobile devices in school .....	6
9. Staff using work devices outside school .....	6
10. Training .....	6
11. Monitoring arrangements .....	6
12. Links with other policies .....	6

---

## 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, sex and health 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.

Maintained schools and academies that follow the National Curriculum insert:

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).

All governors will ensure they read and understand this policy.

### **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 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, IT service provider 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
- › 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 headteacher and/or governing body

This list is not intended to be exhaustive.

### **3.4 The IT service provider**

The IT service provider is responsible 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 IT 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 IT systems on a weekly 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 and dealt with
- › 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 IT 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
- › 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 read this policy, and notify a member of staff or the headteacher of any concerns or queries regarding it.

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](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

## 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
- › 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 to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this, as well as using NGOs and private companies, e.g. Google.

## 5. Educating parents about online safety

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.)

It is the school's position, in consultation with the local police force, that parents are primarily responsible for children's actions, online and otherwise, outside of the school day.

## 6.2 Preventing and addressing cyber-bullying

Adapt this sub-section to reflect your school's approach.

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. Teachers discuss cyber-bullying with their classes, and the issue will be addressed periodically in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes relationships, sex and health education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying occurring during school time, 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 internet-enabled devices in school

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.

All pupils and adults in school, with the exception of the site manager, are prohibited from having access to personal internet-enabled devices, except in the staff room and administration areas of school. Adults are expected to lock any personal internet-enabled devices – except smart watches – in lockers in the staff room and administration areas of school, and to switch all internet-enabled smart watches to airplane mode when in the vicinity of pupils. Any staff failing to comply will be subject to disciplinary procedures.

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

Pupils may bring mobile devices into school after prior agreement with their teacher, but are not permitted to use them during school time.

## **9. Staff using work devices outside school**

Staff members using a work device outside school must not install any inappropriate 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 IT service provider.

Work devices must be used solely for work activities during work time.

## **10. Training**

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.

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

## **11. Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety using the CPOMS service.

This policy will be reviewed every two years by the computing lead. At every review, the policy will be shared with the governing body.

## **12. Links with other policies**

This policy is linked to, and should be considered in conjunction with, our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure