Online Safety Policy

Springfield School

Headteacher: **Date:**

Governor: **Date:**

Reviewed: 01.09.2020

Next review: 01.09.2021

Manor Hall
Academy Trust

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Encourage all pupils to develop skills in computing appropriate to their cognitive and communication level
- 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
- Safeguard pupils through the monitoring of the use of technology within school.
- Safeguard pupils by ensuring that they are educated about e-safety issues and appropriate behaviours so that they remain safe and legal online.

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.

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.

All governors will:

- Ensure that they have read and understand this policy
- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date
- Ensure all staff are taught about online safety as part of their regularly updated safeguarding training, and that this is considered as part of the school's overarching safeguarding approach
- Ensure that children are taught about safeguarding, including online safety, through teaching and learning opportunities.

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.

The Headteacher will ensure:

- Children are taught about safeguarding, including online safety, through teaching and learning opportunities.

- Designated Safeguarding Leads are able to understand the unique risks associated with online safety and are confident that they have up-to-date Online Safety training and up-to-date capability required to keep children safe whilst they are online at school
- The designated safeguarding lead has had appropriate training in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

3.3 The designated safeguarding lead

Details of the school's DSL and DDSL 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, ICT provider (Staffs tech) and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents or incidents of cyber-bullying are logged and dealt with appropriately in line with this policy and the 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 board
- Keep up to date with the latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use.
- Engage with parents and the school community on online safety matters at school and/or at home.

3.4 Staffs Tech

Staffs Tech are 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 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

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 and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Give pupils support in the use of digital technologies, including giving them advice on how to stay safe and to monitor their internet use.

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
- 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.

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 in primary schools.

- The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Online safety is also embedded throughout the Computing curriculum and PSHE curriculum.
- All pupils are constantly reminded to speak to a responsible/ trusted adult if they have any online safety concerns.
- We have online safety displays around school and support for children on our school website

Where appropriate pupils will be taught:

- To develop skills in computing appropriate to their cognitive and communication level
- To use technology safely and respectfully, keeping personal information private
- To identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- 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 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 and in information via our website or coffee mornings . 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.)

Cyber bullying can differ from other forms of bullying:

- Through various media children can be cyber-bullied 24 hours a day
- People who cyber-bully may attempt to remain anonymous
- Anyone of any age can cyber-bully
- Some instances of cyber-bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will support pupils to understand what it is and what to do if they become aware of it happening to them or others. We will support pupils to 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 tutor groups, 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.

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 and parents are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Staff will be expected to follow the guidance within the code of contact in additional to the acceptable use of schools ICT system.

8. Pupils using mobile devices in school

Mobile phones are not permitted within Springfield School. Any alternative electronic devices i.e Ipad needs to authorised by the Headteacher and handed into the school office on arrival.

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 Staffs Tech.

9.1 Use of digital and video images

When using digital images, staff should inform and educate pupils (as appropriate) about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

.

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 Guidance on the use of mobile phones by students and young people

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/disciplinary procedure.

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 and DDSL 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety electronically on myconcern.

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
- Guidance on the use of mobile phones by students and young people

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

E-mail and Internet Use Good Practice

Rules for ICT & Mobile Phone Use

We use the school computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- On a network, I will use only my own login and password, which I will keep secret.
- I will not look at, change, or delete other people's files.
- I will not bring CD ROM's, DVD's, Pen Drives etc. to use in school without permission.
- I will only use the computers for school work and homework unless permission has otherwise been given.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

INTERNET PERMISSION FORM

NAME: ……..

CLASS: ……..…..

DATE: ……..

Pupil section

My parents and I have read and discussed the Rules for Responsible Use of the Internet and I agree to follow them.

Pupil signature ……

Parent / Carer section

I have read and discussed rules for Responsible Use with my son / daughter and -

☐ I grant permission for him/her to use electronic mail and the Internet

☐ I **do not** grant permission for him / her to use electronic mail and the Internet

Parent / Carer signature ……