SPRINGFIELD SPECIAL SCHOOL

Online Safety and Acceptable User Policy

Date Reviewed	January 2023
Next Review Due	January 2024

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
- Support the school's policy on data protection

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 refers to, and complies with the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Education and Training (Welfare of Children Act) 2021

3. Roles and responsibilities

3.1 The Governance - Local Academy Board [LAB]

The LAB has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. Monitoring will be completed through receiving annual reports.

All LAB members 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 2)

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 [DSL] and Deputies

Details of the school's Safeguarding Team are set out in our child protection and safeguarding policy.

A member of the Safeguarding Team is the ICT Lead and 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, Technical Support Provider 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
- Updating and facilitating 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 reports on online safety in school to the headteacher and/or LAB

This list is not intended to be exhaustive.

3.4 The ICT Lead and Technical Support Provider

The school's ICT Lead and technical support provider manages access to the school's ICT facilities and materials for school staff. This includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

The ICT Lead and technical support provider are responsible for:

- Putting in place appropriate filtering and monitoring 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 (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's anti-bullying policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including supply 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 are closely monitored when accessing the internet.
- Working with the member of the Safeguarding Team 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 logged and dealt with appropriately in line with the school's anti-bullying policy
- Embedding internet safety messages wherever possible

This list is not intended to be exhaustive.

Personal Social Media Accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times. This includes ensuring robust privacy settings are in place and that any private social networking sites / blogs that they create or actively contribute to are not confused with their professional role in any way. Staff should take care when posting to any public websites (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school, even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, staff must not post comments on websites that may appear as if they are speaking for the school
- Staff should not post any materials that can be clearly linked to the school, that may cause damage to the school's reputation
- Staff should not post materials clearly identifying themselves, another member of staff, or a pupil that could potentially be used to embarrass, harass or defame the subject

Emails

- The school provides each member of staff with an email address.
- This email account must only be used for work purposes only. All work-related business should be conducted using the email address the school has provided.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

- Staff must take extra care when sending sensitive or confidential information by email.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the headteacher immediately and follow our data breach procedure.

3.6 Parents / Carers

Parents / Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents / Carers can seek further guidance on keeping children safe online from the school website and 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
- CEOP 'thinkUknow': https://www.thinkuknow.co.uk/
- NSPCC – https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- NSPCC SEND - https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-safety-families-children-with-send/
- NSPCC - https://www.ceop.police.uk/safety-centre/
- Parent Zone - https://parentzone.org.uk/
- BBC Staying Safe - https://www.bbc.com/ownit/curations/staying-safe
- National online safety - https://nationalonlinesafety.com/resources/platform-guides/
- Internet Matters SEND - https://www.internetmatters.org/inclusive-digital-safety/advice-for-parents-and-carers/supporting-children-with-send/
- Internet Matters - https://www.internetmatters.org/schools-esafety/parent-online-support-pack-teachers/
- Mencap - https://www.mencap.org.uk/sites/default/files/2016-11/Internet-Safety-web-2016.pdf

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).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, including where appropriate:

- identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Using technology safely, respectfully and responsibly
- Keeping personal information private
- Recognise acceptable and unacceptable behaviour

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

The school may 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.

Where class teachers or class line managers feel it is appropriate a pupil may be asked to sign appendix 1.

5. Educating parents / carers about online safety

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

Online safety will also be covered during parents / carers' evenings where appropriate.

If parents / carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the responsible person from the Safeguarding Team.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. The Management of Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. If this does happen it must be reported immediately and used as a learning opportunity for our pupils on how to access suitable content and what to do should inappropriate content appear on the screen.

7. Cyber-bullying

7.1 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's anti-bullying policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure where appropriate 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 tutor groups, and the issue may 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 Citizen (PSHCE) education, and other subjects where appropriate.

All staff, LAB members 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 shares information on cyber-bullying with parents / carers 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's anti-bullying 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 Safeguarding Team 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.

7.3 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.

8. Acceptable use of the internet in school

All staff, volunteers, LAB members, and when appropriate pupils, 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.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but must use them appropriately and with teachers permission. Some pupils use AAC devices, these devices may be used to take photos, videos and audio recordings of staff, volunteers or other pupils to support their communication and education. Staff will monitor their use in school and ensure that they are not used for reasons other than communication and education.

10. 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.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. This may include the confiscation of a device.

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.

12. 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, bulletins and staff meetings).

The DSL and deputies 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.

LAB Members 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.

13. Monitoring arrangements

The member of the safeguarding team logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually or earlier if necessary in line with national and/or local updates by the ICT lead and Safeguarding Team deputy DSL. At every review, the policy will be shared with the LAB.

14. Links with other policies

This online safety policy is linked to our:

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

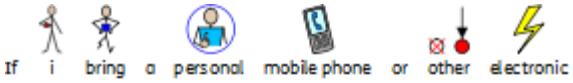
Appendix 1

Acceptable use of ICT + and internet agreement.

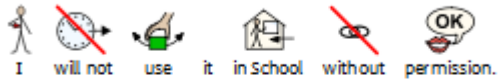
Name .....

When using the schools ICT systems + and accessing the internet in school, i will not.

- Use them without a member of staffs permission
- Access inappropriate web sites
- Accessing social networking sites unless expressly allowed as part of a lesson
- Use chat rooms
- Open any attachments in emails or follow any links without first checking with a member of staff.
- Use inappropriate language when communicating online
- Give my personal information to anyone without permission from a member of staff.
- Arrange to meet anyone offline without permission from a member of staff.


If i bring a personal mobile phone or other electronic


device to school.

- 
I will not use it in School without permission.

- 
I will use it safely, respectfully and responsibly

- 
I agree that school may monitor my device.

- 
I will let a member of staff know if i


find anything that might upset or harm me or


others.


I agree to the rules of the acceptable use of ICT and and


internet agreement.


Signature .....


Date .....


Teacher .....


Date .....

Appendix 2: acceptable use agreement (staff, LAB members, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, LAB members, volunteers and visitors	
Name: **Role: staff member/ LAB member/volunteer/visitor:**	
When using the school's device, ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • 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 • Share my password with others or log in to the school's network using someone else's details	
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 agree that the school will monitor the websites I visit. 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 ICT 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/LAB member/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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, LAB members and visitors?	
Are you familiar with the school's acceptable use agreement for pupils?	
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? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**