



Fairfield Spencer Academy Online

Safety Policy

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 Principals 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.

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

The policy should be read in conjunction with the [Spencer Academies Trust Filtering and Monitoring Policy](#) in relation to 7.3 Managing Filtering.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal 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 Safeguarding Governors also oversee online safety.

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 Principal

The Principal 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 deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSLs takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT Leaders and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing board This

list is not intended to be exhaustive.

3.4 The ICT Leaders

The ICT Leaders are responsible for checking systems in place are appropriate (overseen by AiT Service Providers), which are:

- updated on a regular basis (using the 360 self-review tool) and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- 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, along with the DSL, that any online safety incidents are logged 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 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 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 Principal 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

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. If appropriate, they will be expected to agree to the terms on acceptable use.

4.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. At Fairfield Spencer Academy we follow a programme provided by National Online Safety. Our online safety provision is also taught through our broad and balanced curriculum where relevant: including through our SCARF 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

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 website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings throughout the academic year.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSLs.

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

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 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. 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/SCARF, 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.

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.

7.1 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.

7.2 Social networking and personal publishing

The school will block / filter access to social networking sites for pupils.

Newsgroups will be blocked unless a specific use is approved.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Our pupils are asked to report any incidents of bullying to the school – please see the Behaviour Policy.

School staff are advised not to add children as 'friends' if they use these sites.



7.3 Managing filtering

The school will work with the LEA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, E-Safety Coordinator or Principal.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering and Monitoring at Fairfield Spencer Academy.

- Monitoring software deployed on all school devices via Smoothwall
- Monitoring acceptable use of devices - alerts to DSL/Principal
- Filtering software is Fortinet
- Constantly filtering out and monitoring what children and adults can and can't access on academy devices.

Adults in school – Roles and Responsibilities:

You must report to the DSL if:

- You see or suspect children are accessing unacceptable content;
- You know that unacceptable content can be accessed;
- You are teaching content that could cause a spike in logs;
- You are aware of failure or abuse of the system;
- You perceive there to be unreasonable restrictions;
- You become aware of abbreviations/misspellings that allow access to unacceptable content.

7.4 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material.

Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.

The sending of abusive or inappropriate text messages outside school is forbidden.

Staff will use a school phone where contact with pupils is required.

Staff should not use personal mobile phones during designated teaching sessions.

8. Pupils using mobile devices in school

Pupils in years 4, 5 and 6 may bring mobile devices into school if they are walking to and from school unaccompanied, but are not permitted to use them during school day. All mobile phones must be turned off on entry onto the school premises and turned on only when leaving the school premises. All mobile phones must be handed in at the start of the day and are kept securely in the office or classroom.



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 the ICT Leaders.

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 policies on behaviour and 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 code of conduct and may result in disciplinary action. 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 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.

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 DSLs will monitor safeguarding issues related to online safety that have been reported on CPOMS.

This policy will be reviewed every two years by the Principal. At every review, the policy will be shared with the governing board.

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

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers/iPads) and get onto the internet in school I will:

- Only use websites that a teacher or adult has told me or allowed me to use
- 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
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Save my work on the school network
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

***Parents/Carers: If you do not agree with the acceptable user agreement information, please speak to your child's class teacher to opt out.**



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 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 ICT Leaders 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.

I take full responsibility of IT resources loaned to me by school and understand that if lost or stolen due to negligence, I will be required to fund a replacement.

Signed (staff member/governor/volunteer/visitor):

Date:



Appendix 3: Remote Learning

Online Safety

When your child is accessing remote online learning, it is vitally important that they know how to stay safe. Remote online safety has been taught in school to all children; please take time to revisit this information with your child(ren) at home. Please ensure they know how to raise concerns with the school, [Childline](#), the [UK Safer Internet Centre](#) and [CEOP](#).

At Fairfield we ensure that any use of remote online learning tools and systems are in line with privacy and data protection/GDPR requirements.

- All work will be presented via Class Dojo
- Remote online messages between parents/children and staff will be done via Dojo messaging. No staff will share their private emails with parents or children.
- Live virtual lessons will not be delivered as part of remote online learning at Fairfield. Where required, teachers may film themselves and post these 'lessons/stories' on Class Dojo

Additional support for parents and carers to keep children safe online includes:

- [Thinkuknow](#) provides advice from the National Crime Agency (NCA) on staying safe online
- [Parent info](#) is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Internet matters](#) provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [London Grid for Learning](#) has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Net-aware](#) has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- [Let's Talk About It](#) has advice for parents and carers to keep children safe from online radicalisation
- [UK Safer Internet Centre](#) has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services

Use of Zoom to Support Communication with Teachers and Peers

To support online face-to-face communication, we are using a product called Zoom for our video-calling. We will be using our school account for this, so you do not need to buy anything or create an account.



You can access Zoom via a laptop, mobile phone or a tablet.

For online face-to-face communication, via the Zoom platform, there will be a meeting code and password required. This will be shared with you by a member of staff.

So that identities can be confirmed, when using Zoom we require parents/carers to:

- identify their account using their name
- select join with video and audio

To use the video link just click on it. The browser window will open and the first time you use it, it will ask you to download the software. If you use a Zoom account for another reason, please make sure you log out of that account before your child uses it. This will make sure any settings that you have made in your account do not over-ride any that we have put in place to safeguard your child.

Safeguarding

At Fairfield, we take the safeguarding of your child very seriously and to ensure this, we have put many safeguarding elements in place. Therefore, you will enter a virtual waiting room when you click the link. The teacher leading the call will enable you to enter when the meeting starts. Please ensure your video is on, so that we can see you.

When we make the video call please make sure the computer is in a suitable place (not in a bedroom or bathroom for example) and the background is clear, showing just the wall perhaps.