Online Safety & Acceptable Use

February 2021

Agreed: February 2021 **Review Term: Spring 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

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 DfE'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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head teacher 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 Suzie Howard, Safeguarding 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 4)

3.2 The head teacher

The head teacher 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 as relevant job descriptions.

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

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, IT support company (TSI) and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on the Incident log on Microsoft Forms 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 head teacher and/or governing board
- Review monitoring reports provided by Securus on a fortnightly basis.

3.4 IT support company

The IT support company (TSI), under direction of the DSL 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 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 monthly basis.
- Ensure that filtering is in place that blocks access to potentially dangerous sites and, where possible, prevents 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 IT systems and the internet (appendix 3 & 4, and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 and bullying policies

3.6 Parents

Parents are expected to:

- Notify a member of staff or the head teacher 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 IT systems and internet (appendices 1 and 2)
- 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
    - Healthy relationships – Disrespect Nobody

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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the RSHE curriculum. The Assistant Head teacher for Personal Development is responsible for ensuring the curriculum includes the following:

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 time pupils leave Fielding Primary School they 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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in half-termly 'Latest News' articles on the school website and via the bulletin. There will also be reference materials on for parents on our online safety page on our 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 class teacher or the DSL.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying (also known as online 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 and bullying policies.)

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 class during RSHE and computing lessons.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

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 highlights information 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 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 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 and the school's COVID-19 risk assessment.

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, parents, staff, volunteers and governors are expected to read our agreements regarding the acceptable use of the school's IT systems and the internet (appendices 1-4). If pupils, parents, staff, volunteers or governors are not willing to follow the acceptable use guidelines then they must raise this with the head teacher or DSL. Acceptable use agreements will be shared in the following ways:

- Pupils and parents; posted to our website and published for pupils in their reading journal. Class teachers will take time to go through these with pupils at the start of a school year.
- Staff, published in the staff handbook.
- Visitors, including visiting teachers, and volunteers will receive a copy on arrival be expected to read and agree to
- Members of the Governing Board will be provided a copy as part of this policy

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils in Years 4, 5 and 6, who may be walking to and from school by themselves, may bring mobile devices into school, but are not permitted to use them during the school and extended school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil will trigger sanctions in line with the school behaviour policy, and may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Asking TSI to install anti-virus and anti-spyware software
- Making the device available to TSI for software and operating system updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT and internet acceptable use agreements. 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 IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Ealing 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.

A risk assessment is in place for the use of IT for remote learning. See Appendix 5.

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 through the Friday staff briefing and Looking Ahead staff bulletin.

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

This policy will be reviewed every 3 years by the DSL. 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 code of conduct
- Data protection policy and privacy notices
- Complaints procedure

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

Acceptable use of the school's IT systems and internet: agreement for pupils and parents/carers

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- 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
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- 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.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's IT systems and internet: agreement for pupils and parents/carers

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 educational 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 consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will give it to my class teacher to store securely,
- I will not use it during school time, clubs or other activities organised by the school, without a teacher's permission

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

Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff)

Acceptable use of the school's IT systems and internet: agreement for staff,
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 unless this is for work purposes • 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 • Share confidential information about the school, its pupils or staff, or other members of the community unless required to do so for work purposes and then only through encrypted channels of communication. • 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
During school hours 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. Outside of school hours if I use this a work device for personal use I will not access inappropriate material, including but not limited to, material of a violent, criminal or pornographic nature. Any attempt to do this will be a breach of the staff code of conduct and will result in disciplinary action. 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 manager 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.

Appendix 4: acceptable use agreement (governors, volunteers and visitors)

Acceptable use of the school's IT systems and internet: agreement for governors, volunteers and visitors	
Name of 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 unless this is for work purposes • 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 unless required to do so for work purposes and then only through encrypted channels of communication. • 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 for educational purposes, 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 manager 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 (governor/volunteer/visitor):	**Date:**

Appendix 5: Risk assessment for remote learning

Please check for the most up-to-date version

Risk assessment for remote learning v2 Feb 2021

	Risk	Mitigation
1.	Inappropriate behaviour or conduct from parents	Remind adults about online conduct. Remove from call. Let HT/DHT know via Teams.
2.	Inappropriate behaviour or conduct from pupils for example: • sharing explicit content • bullying/harassing each other • inappropriate chat on the class post	Clear expectations in place. Follow behaviour system, remind pupils of expectations. Repeated behaviour 'mute' child speak to parents. Microsoft Teams is configured to limit when pupils can chat during lessons and who they can chat with. We'll share these resources with staff, pupils and parents: • UK Safer Internet Centre, where they can report harmful content • Educate Against Hate for safeguarding from radicalisation, building resilience to extremism, and promoting shared values • The National Crime Agency's Child Exploitation and Online Protection Command for advice on reporting online abuse
3.	Unauthorised recording by pupils, parents, or staff	Ask parents, pupils not to record meetings. Log on concern form if this happens.
4.	Unauthorised sharing of content	Check permissions before content is shared. e.g. copyright.
5.	Inappropriate dress, conduct, or location	Clear guidance sent out to all pupils and staff on expectations. In the event this occurs, teacher to switch off child's camera. Any breach of these – a reminder sent to pupils, log on concern form.
6.	Unauthorised people invited into the video call	Class teams have no access to guest users.
7.	Data breach. For example, showing pupils on camera without permission, sharing personal data	Check permissions. No recording of pupil meetings if permission for sharing image not granted. Log on concern from.
8.	Data breach showing confidential information whilst online	Remind staff of GDPR rules. Report to DPO. Complete incident log.
9.	Unauthorised lessons that LT are unaware of	Leadership team are part of every class team, all meetings to be scheduled through class channel.
10.	Accidentally being online early or afterwards without being aware (pupils)	Lobby to be set for all meetings, teacher to log off (end call for pupils) last.
11.	Unauthorised chats or video whilst monitoring adult is offline	Pupils cannot start video calls. Chat to be monitored and point 2 above.
12.	Use of Microsoft Teams by unauthorised staff or untrained staff	Access by username and password authentication only. Staff leavers removed from system when contract expires. Induction for users when username and password issued.
13.	Staff and/or pupils viewing or hearing inappropriate content, either in an individual's environment, on their person or on their screen	If staff and pupils have their cameras on, they will be asked to: • have a neutral background, if possible • avoid being situated in their bedroom • dress like they would for school • use polite and professional language staff will be asked to: • blur their background or have a plain backdrop • if sharing on YouTube have auto play turn off and use You-Tube so advert free, appropriate content only • double check that any tabs they have open in their browser would be appropriate for a pupil to see, if they're sharing their screen • adults to check content of any shared video/PowerPoint/other ahead of time (e.g. YouTube) only share school based or Oak based lessons
14.	1-to-1 sessions	sessions will be assessed case-by-case basis whether a session needs another adult present 1-to-1 sessions will only be run where appropriate and necessary. 1-to-1 sessions will need approval by the leadership team before taking place. 1:1 sessions should be recorded if a parent is not present (eg learning mentor session)
15.	Parents and pupils not knowing how to keep pupils safe online	Half termly Latest News articles will be posted for parents with information on how to keep their children safe online.
16.	What action is to be taken if a disclosure/concern or allegation is raised by pupil whilst online?	Use MyConcern. Report using usual school systems.
17.	How will concerns be raised about any Microsoft Team live issues by pupils, parents or staff?	Raise with senior leaders through Microsoft Teams (staff, pupils) via admin email (parents)
18.	Errors, mistakes, or concerns should be self-reported. How should this be done?	Report logged on incident report log, Microsoft forms.