Online Safety Policy

Fairview Community Primary School

Key Details

The Designated Safeguarding Lead:
Karin Tillett
Computing Lead Teacher: Philip Hammett
Technical Management/Support: BCTec

Reviewed: February 2026
Review Due: February 2028

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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
- 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 the Equality Act 2010 and reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, investigating 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 body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of the child protection and safeguarding training and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will co-ordinate meetings with appropriate staff to discuss online safety, monitor recorded incidents relating to online safety as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Chris Woods.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSLs 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:

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the BCTech to make sure the appropriate systems and processes are in place
- Working with the Computing Lead, the school's technical support provider (BCTec) and other staff, as necessary, to address any online safety issues or incidents
- Managing online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with the policy
- Ensuring that any incidents of cyber-bullying are logged (CPOMS) and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The Network

The school's network is overseen by the school's technical support provider (BCTec). Note:

- The filtering and monitoring is provided by Medway.
- The web filtering is set for schools by Medway but it is a granular system and the school's technical support provider (BCTec) can edit/adjust/flag up any potentially harmful or inappropriate sites/content, including terrorist and extremist material and online chat. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- 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
- The school uses an additional monitoring/filtering system (presently- Smoothwall) that flags up inappropriate online use. Any alerts are sent directly to the DSL/headteacher who will then carry out an investigation.
- Ensuring that any online safety incidents are logged (CPOMS) 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

3.5 All staff and volunteers

All staff, including contractors, 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 (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendices 3 and 4)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing in the appropriate way.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (CPOMS) 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/Anti-bullying policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

- Know that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 3 and 4)
- 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 resource sheet – 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 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 1).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 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 (KS) 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

4.1 Fairview's Approach to children's use of social media

The safe use of specific social media platforms will also be covered.

The overall approach is indicated below:

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will highlight this throughout our teaching, along with the rationale behind why such sites are inappropriate for the primary age range.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Without directly referencing any age-restricted social media sites, Learners will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the setting and externally.

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 initial parents' meetings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 DSLs.

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 1 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 a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

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.

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching

and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

This information is also contained in the school's acceptable use policy.

7. Publishing images and videos online

7.1 Consent forms

- All parents of pupils at Fairview are asked to sign a consent form to gain permission to publish photographs in public places (including websites) - please see Appendix 5.
- If parents or carers disagree over consent for a child, it will be treated as if consent has not been given.

7.2 Use of images

Parents and carers

- The school will include in the first newsletter of every academic year a reminder that photographing and videoing of school events by parents and carers is permitted, unless stated otherwise in the invitation. Parents are reminded that under no circumstances are any images of Fairview pupils to be displayed on any social networking site.
- Those parents, carers and volunteers who are in the school to help with assisting children to dress or change will not be allowed to take photos or videos during this time.

Schools

- The school will not publish any photographs of children whose parents have withheld their permission.
- No personal devices should be used for taking photographs of Fairview pupils.
- Photographs of pupils must not be downloaded and saved on to personal devices.

Children who should not be identified

- Every effort will be made by the school to prevent capturing of the image of any child who should not be identified.
- If the school becomes aware that a child who should not be identified or who should not be photographed has been photographed, the photograph, electronic record or negative will be destroyed.
- If the school does not hold the photograph, electronic image or negative, the school will make every effort to contact those who do hold them and request their destruction.
- If the image cannot be destroyed or if the school cannot stop publication of an image of a child who should not be identified, the school will immediately contact the parents/carers of the children involved and inform them the image has been produced.
- If the pupils concerned are Looked After Children, the school will immediately contact the children's social workers.

7.3 Media photographing and filming

- If the media are invited into school for publicity purposes, the school will check before the event whether any of their pupils should not be identified.

7.4 Video conferencing

- Where parents have asked that their children's images should not be included in video conferencing every effort will be made to avoid this.
- If the school becomes aware that a child who should not be identified has taken part in video conferencing, the school will immediately contact the parents/carers/social workers of Looked After Children to inform them.

7.5 Pupils

- Pupils are taught about how images can be manipulated in their eSafety education programme, and are taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.
- Pupils are advised to be very careful about placing any personal photographs on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school.
- Pupils are taught about the need to keep their data secure and what to do if they are subject to online bullying or abuse.

7.6 Guidance for parents and carers

- Written guidance is given to parents/carers to the effect that any images must be taken for personal use only and that images including others must not be put on the web/internet, and that if they are, Data Protection legislation may be contravened.
- A copy of the 'using your camera and video courteously' code is given to all parents/carers when their child joins Fairview. Please see Appendix 6.
- People with no connection to our school will not be allowed to photograph or video – staff will question anyone they do not recognise who is using a camera and or video recorder at events and productions.

8 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Fairview recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Fairview will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

9. 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 1/3-4). 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 1/3-4. Further information can be found in the school's acceptable use policy.

10. Pupils using mobile devices in school

Only pupils in Years 5 and 6 are allowed to bring in devices as they may be required for walking to

and from school. Children are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school.

Pupils will hand the mobile device into their class teacher at the beginning of the day where they

are placed in a locked drawer/box. Pupils must adhere to the school's agreement for mobile phone use (see Mobile Phone Policy).

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

11. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. Use of Office 365-OneDrive (Fairview's subscription) is a key focus.

General security steps relating to devices outside school 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)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest 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 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing Lead/the school's technical support provider (BCTec).

14. 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 as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety.

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.

15. Monitoring arrangements

The DSL/headteaher monitors behaviour and safeguarding issues related to online safety (via CPOMS).

This policy will be reviewed every two years by the Computing Leader of Learning. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to the following policies (click here for our policies page):

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Mobile phone policy
- Acceptable Use Policy
- Social Media Policy

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Fairview Community Primary School

Acceptable Use Agreement: All Staff, Volunteers and Governors

This Acceptable Use Agreement covers use of all digital technologies in school: i.e. email, Internet, network resources, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems I have access to.
- I will ensure all documents, data etc. are printed, saved, accessed and deleted / shredded in accordance with the school's Data Security Policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system for any school business, and will ensure e-mails are encrypted when they contain information of a sensitive nature.
- I will only use the approved email system and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head Teacher or School Business Manager.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will follow the school's policy on use of personal mobile phones / devices at school
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Fairview's Designated Safeguarding Lead / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead at the school.
- I understand that the levels of filtering in place by LGFL are set to ensure that children are safe from inappropriate, terrorist and extremist material when accessing the Internet at school, and will alert senior members of staff and the child protection officer if I feel any child may be exposed to such material intentionally or otherwise.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head Teacher at their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only*: I will embed the school's e-safety / digital literacy curriculum into my teaching.

Acceptable Use Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a ‘safe and responsible digital technologies user’.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Appendix 2: online safety training needs – self audit for staff

Core Template

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
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?	

Appendix 3: EYS and KS1

Fairview Community Primary School

Use of the Internet by Pupils

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I always tell an adult if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I know that if I do not follow the rules, sanctions could follow

Pupil Agreement

We have read and understand the school rules for Responsible Use of the internet.

Name of Class:

Date:

Fairview Community Primary School
Use of the Internet by Pupils

- I only use the internet when an adult is with me for my school work or homework
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I always tell an adult if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I know that if I do not follow the rules, sanctions could follow

Pupil Agreement

I have read and understand the school rules for Responsible Use of the Internet.

Name of Pupil:

Pupil Signature:
Date:

Appendix 4: KS2

Fairview Community Primary School

Use of the Internet by Pupils

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always ask permission from an adult before using the internet
- I only use websites, homework apps and search engines that my teacher has chosen
- I use school computers for school work, unless I have permission otherwise
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher has allowed me to

Understand

- I understand that the school/ internet filter is there to protect me, and I will not try to bypass it
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online
- I know that if I do not follow the school rules then sanctions could follow

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher

- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away

Pupil Agreement

I have read and understand the school rules for Responsible Use of the Internet

Name of Pupil:

Pupil Signature: Date:

Appendix 5

Fairview Community Primary School Consent Form for use of images of children

The school will include in the first newsletter of every academic year a reminder that photographing and videoing of school events is permitted by parents and carers, unless stated otherwise in the invitation. Under no circumstances are any images of Fairview pupils to be displayed on any social networking site.

Occasionally, we may take photographs, or make video or web cam recordings, of the pupils at our school. We may use these images on displays around the school, in our school prospectus, or in other printed publications that we produce, as well as on our website and Twitter feed.

Sometimes the media (papers, radio or television), Medway Council or external organisations that Fairview works with may visit our school and interview and/or take photographs, videos, or sound recordings of our pupils. These images may then be published in the local or national press, these organisations' own websites and publications.

We will not provide personal details or full names (which means first name *and* surname) for any publication.

Please note that websites can be seen throughout the world, and not just in the United Kingdom.

Please answer the question below, then sign and date the form where shown, and return the completed form to the school as soon as possible.

Please circle

Do you give consent, for your child, as detailed above? **Yes / No**

Parent's or Carer's signature: _____ Date: _____

Name (in block capitals): _____

Address _____

Name of the child:

Telephone Number:

Appendix 6

Fairview Community Primary School - using your camera and video courteously

A guide for parents and carers who wish to use photography and/or video a school event

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves. By following some simple guidelines we can proceed safely and with regard to the law.

Please remember that parents/carers and others, attend school events at the invitation of the school.

The Head Teacher and governors have the responsibility to decide if photography and videoing of school performances is permitted.

The Head Teacher and governors have the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.

Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos must not be sold and must not be put on the web/internet. To do so would likely break Data Protection legislation.

Recording or photographing other than for your own private use would require the consent of all the other parents/carers whose children may be included in the images and, for good reasons, some parents/carers may not want their children to be photographed.

Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

Parents and carers must not photograph or video children changing for performances or events

If you are accompanied or represented by people that school staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

Remember that for images taken on mobile phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.