Online Safety Policy

This policy relates to the Curriculum Policy and the Safeguarding Policy

Policy Written By: Sasha Palmer

Policy Reviewed: 26th September 2021

Review Date: September 2022

Policy: Curriculum; Safeguarding

Governors:

Finlay Community School

Online Safety Policy

1: Introduction

Technology is an important and essential part of the learning experience at Finlay Community School. We are committed to ensuring that our children leave with the skills and knowledge that will help them to thrive in our digital age. We have an ICT suite, a set of laptops and one IPad per class, which are used most days.

The teachers use the internet daily with the children. It is therefore also vital that we teach children how to use this valuable resource safely. This policy will appreciate that all children have access to smart phones, IPads and computers at home and within school. It promotes the use of these technologies whilst committing to keeping our children aware of and safe from the potential risks. We will demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. This online safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

1.1: Aims of this policy

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, 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

1.2: 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, Health and Sex Education (RSHE)
- 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.

2: Internet Safety at Finlay

At Finlay, we take internet safety very seriously. We are part of the South West Grid for Learning (SWgfl) therefore we benefit from their internet filters. As the digital world constantly changes, alongside the information that is accessible on the internet, staff and the Computing Subject Leader continuously review the content our children can access, and address this accordingly. If we find any content that is inappropriate, we can email it to our IT Technician, who will solve this either in school or remotely. We are also working towards an E-safety Mark using the 360 degree safe auditing tool. In addition to this, we subscribe to the Boost+ SWgfl platform which allows staff to access e-safety materials, training and information for parents as and when necessary. Websites such as Google are subject to filters and where the images search has partial filters; children are taught how to search using appropriate vocabulary. Children are taught to take responsibility for appropriate internet use in school.

3: Teaching Internet Safety.

We ensure as a staff team that Internet Safety is thoroughly taught across the school, and this is progressive. We have a 'planning matrix' which is used as a teaching and learning tool across school (see our Curriculum policy for more information). On the Computing Matrix, the knowledge, skills and understanding that should be taught in regards to e-safety is mapped out from pre-school through to year 6, and is progressive, with key content being revisited as appropriate. This knowledge, skills and understanding is sometimes taught in isolation, through computing lessons or as part of our Relationships and Health Education (RSHE) program. The units that staff need to cover with their class are in line with SWGfL E-Safety teaching units and are in line with the Teaching Online Safety in School guidance released by the DfE in 2019. We use a scheme of work called Switched on Computing to deliver our computing curriculum, and messages of e-safety are interwoven all the way through. The Computing Subject Lead works alongside the Curriculum Lead to ensure there is coverage of these essential knowledge, skills and understanding across school. In addition to teaching the relevant knowledge, skills and understanding, we also strive for positive mental health and wellbeing to underpin everything we do, which is in line with our core SMILE values (as outlined in our Curriculum policy). We therefore monitor the effects that the internet and social media has on our pupils, and explicitly teach them about this and how to recognise these feelings in themselves.

We also participate in online safety national days, and work collaboratively with our local policing team to deliver key messages related to internet safety.

We also work alongside parents and carers in our community to support them in ensuring their children are safe online. Each month, we send out an online safety newsletter, which includes the most up to date information about online safety and apps/games.

3.1: What to teach

Pupils will be taught about online safety as part of the National Curriculum. The text below is taken from the National Curriculum Programmes of Study for computing, and outline what is taught in Key Stage 1 and Key Stage 2. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education. **ALL** schools have to teach:

- Relationships education and health education in primary school: We deliver this through the Jigsaw programme, with sessions taught every week across the whole school.

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
- 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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Safer Internet Day

Every year, we participate in Safer Internet Day, however we do ensure that our e-safety teaching is not limited to just this day. As part of Safer Internet Day, we work alongside our local Police Community Support Officers, who come in and deliver sessions to the pupils

Underpinning knowledge and behaviours that the curriculum covers include:

3.1.1: How to evaluate what they see online

This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. At Finlay, we help pupils consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

3.1.2: How to recognise techniques used for persuasion

This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

At Finlay, we help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
- Techniques that companies use to persuade people to buy something,
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design);
- Criminal activities such as grooming

3.1.3: Online behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour look like. At Finlay, we teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We also teach pupils to recognise unacceptable behaviour in others. At Finlay, we help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- Looking at how online emotions can be intensified resulting in mob mentality,
- Teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online;
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

3.1.4: How to identify online risks

The potential risks are:

- child sexual abuse
- exposure to radicalising content
- youth-produced sexual imagery ('sexting')
- cyberbullying
- exposure to age-inappropriate content, such as pornography
- exposure to harmful content, such as suicide content

This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action. At Finlay, we help pupils to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online,
- Discussing risks posed by another person's online behaviour,
- Discussing when risk taking can be positive and negative,
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example.

- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with;

- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

3.1.5: How and when to seek support

This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

At Finlay, we can help pupils by:

- Helping them to identify who trusted adults are in school,

- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline. This links to our safeguarding and child protection policy, which is in line with Keeping Children Safe in Education.

- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

3.2. Cyber-bullying

3.2.1 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.)

3.2.2 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.

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 Relationships and Health Education (RSE), and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

3.2.3 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

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

3.3. 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. 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.

3.3:1 Expectations of pupils when using the Internet

All pupils are expected to read and agree the Internet Agreement.

- At Finlay, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc, USB stick or CD Rom should be brought in from the home for use in school. This is for both legal and security reasons.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made.
- Pupils consistently choosing not to comply with these expectations will be warned and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a letter to parents and withdrawal of privileges.

3.3.2. 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)

- 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.

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 headteacher/ DSL/ ICT Manager.

3.3.3. 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. 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.

4. Reporting E-Safety Concerns

We work closely with the children and our parents to develop an ethos in school where by the children and parents feel they can come to us with any e-safety concerns. We investigate these fully and deal with them appropriately, in line with our safeguarding and child protection policy. When incidents have happened outside of school, we inform parents what has happened and we explain which other ways they can seek help outside of school: e.g. reporting on apps and contacting the police. We also work closely with our local Police Community Support Officers who help us to do this. If incidents crop up that involve wider issues e.g. the use of a particular app, we plan time into our curriculum to address this with the relevant children/classes to aim to limit this happening again. We also send home guidance where needed. All e-safety incidents are to be recorded and logged on CPOMS.

4.0: Working alongside our parents/carers

At Finlay, we understand that a key way of delivering e-safety messages and ensuring children are safe online is to involve our parents. As previously mentioned, we live in a digitally advancing world, with things changing by the day. Our parents/carers play a crucial role in ensuring their children understand the need to use the internet/mobile devices in an appropriate way. We keep our parents updated regularly with regards to:

- Ways to stay safe online
- How to use parental controls on different devices
- New apps that are available
- Other information we deem appropriate and relevant.

We send out help sheets to our parents if we know their children are accessing certain apps or if they ask for more information. We also provide regular information on our Facebook page for parents to access.

Parents and carers are also encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

- their children's personal devices in the school

4.1: Our School Facebook Page

At Finlay Community School, staff regularly use our school Facebook page to communicate information to parents. All parents can access the site, and must give permission for photographs/videos of their child to be shared. Should any parent wish for their child's/children's photographs not to be shared, this is noted and all staff are aware of this to avoid it from happening. Staff do not communicate personally with parents on Facebook, and should only use the school Facebook page for professional communication only. Parents' comments are closely monitored and reviewed regularly to ensure they are appropriate.

Parents Reporting E-Safety Concerns (Guidance from Keeping Children Safe Online)

4.2. Concerns Regarding Radicalisation

If there are any concerns that any family member, friend or loved one is being radicalised, you can call the police or 101 to get advice or make a Prevent referral, so that they can get safeguarding support. Support is tailored to the individual's needs and works in a similar way to safeguarding processes designed to protect people from gangs, drug abuse and physical and sexual exploitation. Receiving support through Prevent is voluntary, confidential and not any form of criminal sanction. If you need further help, you can also contact your local authority safeguarding team. (Mentioned in Keeping Children Safe Online)

Educate Against Hate Parents' Hub provides resources and government advice for parents and carers on keeping young people safe from extremism, including online.

Let's Talk About It provides support for parents and carers to keep children safe from online radicalisation.

Any member of the public can report terrorist content they find online through the GOV.UK referral tool. More information about what to report and what happens when you make a report can be found on the Action Counters Terrorism campaign.

4.3. Sexting

If you are worried about your child sending nude images or videos (sometimes referred to as 'youth-produced sexual imagery' or sexting), NSPCC provides advice to help you understand the risks and support your child.

If your child has shared nude images, Thinkuknow by National Crime Agency-CEOP provides advice on talking to your child and where to get help.

4.4. Age Inappropriate Content and Parent Controls

If you have downloaded new apps or bought new technology to help stay connected at this time, remember to review and adjust privacy and safety settings if you or your child is signing up to a new online service.

Internet Matters has provided step-by-step guides on how to set up parental controls so that you can control what content your child can access online.

The UK Safer Internet Centre has developed guidance on how to switch on family-friendly filters to prevent age-inappropriate content being accessed on devices in your home.

The NSPCC provides more information for parents or carers with concerns about their child seeking inappropriate or explicit content online.

4.5. Mental Health and Wellbeing

If you are worried about your child's mental health, the government has published guidance for parents and carers on supporting children and young people's mental health and wellbeing during the coronavirus (COVID-19) outbreak.

If you are worried that someone you know is suicidal, including your child, Samaritans provides advice on how you can support others.

5: Roles and Responsibilities

At Finlay, we understand that it is important to work collaboratively and our online safety policy effects everybody. Below are the key roles of different members of staff:

5.1: Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, who receive regular information about online safety incidents and monitoring reports. The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will:

- hold regular meetings with the Online Safety Co-ordinator/Computing Subject Leader, Curriculum Lead and Designated Safeguarding Lead
- discuss online safety and monitor online safety logs as provided by the DSL
- regular monitoring of filtering logs
- reporting to relevant Governors

All governors will:

- Ensure 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
- 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.

5.2: Executive Head Teacher, Head of School and other Senior Leaders

- Have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the Online Safety Co-ordinator and Computing Subject Leader.
- Should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Will ensure that the current system in place allow for monitoring of issues and support of those in school who carry out the internal online safety monitoring role.

5.3: 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 headteacher in ensuring that staff understand this policy, and that it is being implemented consistently throughout school
- Working with the headteacher, ICT manager, Computing Lead and senior leaders as necessary to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy. These should be recorded on CPOMS
- 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 headteacher and/or governing board.

5.4: E-Safety Coordinator, Curriculum Leader and Computing Subject Leader

The E-safety Coordinator is a shared role between the Computing Subject Leader and the Designated Safeguarding Lead. They:

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice for staff.
- Liaise with school technical staff
- Receive reports of online safety incidents and ensures there is a detailed log of incidents to inform future online safety developments (recorded on CPOMS).
- Meet regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- Prepare resources for parents to support with online safety at home.

5.5: The ICT Technician/Manager

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring of the school's ICT systems regularly.
- Blocking access to potentially dangerous sites, and where possible, preventing the downloading of potentially dangerous files.

5.6: Teaching and Support Staff

re responsible for ensuring that:

- They maintain an understanding of this policy and implement it effectively
- They have an up to date awareness of online safety matters
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- Work with the DSL to ensure that online safety incidents or incidents of cyber-bullying are logged and dealt with appropriately; they report any suspected misuse or problems to the Designated Safeguarding Lead.
- They respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintain an attitude of 'it could happen here'.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Potential or actual incidents of grooming

5.7: Parents

Are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the school's acceptable use policy.
- Read the monthly online safety newsletter that is emailed out.

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

6. 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).

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 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.

7. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. The recorded information will be uploaded to CPOMS.

8. 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
- Acceptable Use

Approved: (the below signatures are proof of policy approval)

Signed: Sasha Palmer	Author Date: 27.09.21
Signed: Michelle Bryce (DSL)	DSL Date:
Signed:	Head teacher Date: ----------
Signed:	Governors Date: ----------

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET

AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

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
- 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 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 ICT SYSTEMS AND INTERNET:

AGREEMENT FOR PUPILS IN KS2 AND PARENTS/CARERS

Name of pupil:

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 not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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, 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 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 (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

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?	