E-Safety

Policy Written By: Sasha Palmer

Policy Reviewed: September 2020

Review Date: September 2021

Policy to be taken to Governors: No

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.

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 Pink Curriculum (PSHE) 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. 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.

3.1: What to teach

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching at Finlay is built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches. Teaching must always be age and developmentally appropriate.

Underpinning knowledge and behaviours 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: 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: 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.

3.4: 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
-

3.4.1: 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.

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.

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

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator/Computing Subject Leader, Curriculum Lead and Designated Safeguarding Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors

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: 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.

5.4: Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problems to the Designated Safeguarding Lead.
- 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.
-

5.5: Designated Safeguarding Lead

The Designated Safeguarding Lead and deputies should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with strangers
- Potential or actual incidents of grooming

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

Signed: Sasha Palmer — Author Date: 24.03.2020

Signed: — Head teacher Date: ----------

Signed: — Governors Date: ----------