Online Safety Policy

Geoffrey Field Junior School

Written January 2023
Review January 2025

1. Background and Purpose

1.1 Being able to interact and navigate the online world is an absolute essential skill for pupils as technology does, and will continue to play an important role in their everyday lives. Consequently, schools need to build in the use of this technology in order to equip our young people with the skills to access life-long learning and employment.

1.2 Whilst regulation and technical solutions are very important in mitigating the possibility of pupils finding themselves in dangerous situations online, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

1.3 Computing at Geoffrey Field's covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of information and Communication Technology (ICT) within our society as a whole. Children are no longer passive users of the internet but are active participants, moulding and interacting their online experience.

1.4 Whilst exciting and beneficial both in and out of the context of education, there is no consistent policing of the online world. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

1.5 At Geoffrey Field Junior School, we understand the responsibility to educate our pupils of the risks they will encounter online, teaching them the appropriate behaviours and critical thinking skills they will need to enable them to interact with the internet and related technologies both safely and legally.

2. Roles and Responsibilities

Governing Body

2.1 The governing body is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

2.2 Governors will receive regular information about online safety at the school through the safeguarding link governor.

2.3 Incident and monitoring reports will be fed back to the governing body.

Head Teacher

2.4 As online safety is an important aspect of strategic planning within the school, the Head has ultimate responsibility in ensuring that the policy and practices are embedded and monitored.

2.5 The Head Teacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

2.6 The Head Teacher, with support from the online safety lead, will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

2.7 The Head Teacher is responsible for ensuring that the online safety lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Lead

2.8 The school has a named online safety lead, the role being part of their wider computing coordination. It is the role of the online safety to keep abreast of current issues and guidance from relevant bodies and updating the policy and practices at the school so that it is in line with any future developments.

2.9 The online safety lead takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies.

2.10 The online safety lead will liaise with relevant bodies and the school's technician.

Teaching & Support Staff

2.11 Teaching and Support Staff are responsible for ensuring that they have an up to date awareness of online safety matters and of the current school policy and practices. All teaching and support staff must read and sign the school 'Acceptable Use of IT' policy to confirm they will adhere to the instructions issued.

2.12 If staff observe or suspect any misuse or concerns relating to a child's online behaviour of safety, these must recorded and reported (following the school's child protection policy where appropriate).

Pupils

2.13 Pupils are responsible for using the school ICT systems in accordance with the pupil 'Internet Safety Agreement' and the school's 'Remote Learning' policy.

Parents & Carers

2.14 Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet in an appropriate way. Geoffrey Field takes every opportunity to help parents understand these issues through parents' evenings, literature on the school website and through policies.

2.15 Parents/carers will be encouraged to support the school in promoting good online safety practice and supporting learning online at home.

3. Online Safety in the Curriculum

3.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision.

3.2 Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety forms an essential part of our school's computing curriculum.

3.3 **Educating pupils about the online risks** that they may encounter inside and outside school is key to the online safety curriculum as all of the children will be part of an online community, whether inside or outside of school.

3.4 The online safety curriculum focuses on five key areas of online safety, which are then developed as the pupils move through key stage two:

1.) How to evaluate what they see online
2.) How to recognize techniques used for persuasion
3.) Online Behaviour
4.) How to identify online risks
5.) How and when to seek support

3.5 Online safety teaching is **up-to-date** and involves areas of the internet that the children are using. Staff training is key to ensuring teaching is relevant. The school's Digital Leader team also

3.6 Pupils are aware of the relevant legislation when using the internet such as **data protection** and intellectual property, which may limit what they want to do but also serves to protect them.

3.7 Pupils are taught about **copyright, respecting other people's information, safe use of images** and other important areas through discussion, modelling and appropriate activities.

3.8 Pupils are aware of the **impact of Cyberbullying** and know **how to seek help** if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button.

3.9 Pupils are taught to critically **evaluate online materials** and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum. Children must learn to be discerning when viewing information online and E-safety must help them develop their critical thinking.

3.10 Teaching children to spot the difference between **appropriate and inappropriate behaviour** online and where they can report any concerning behaviour.

3.11 As part of our commitment to online safety, pupils acknowledge and sign the Geoffrey Field's 'Internet Safety Agreement' each year. The agreement outlines the key strands of E-Safety in a child friendly language and is routinely referred when the school's computers and tablets are being used.

4. Supporting Parents with online safety

4.1 Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

4.2 The school/academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Learning Platform
- Parents/carers evenings/sessions
- Internet Safety Day
- Links on our website and parent newsletters

4.3 Parents are also encouraged to seek guidance from the school if they are concerned about an online safety matter.

5. Dealing with illegal activities

5.1 Some internet activity (i.e. accessing child abuse images or distributing racist material) is illegal and would obviously be banned from school and all other technical systems. Other activities (i.e. cyber-bullying) would be banned and could lead to criminal prosecution.

5.2 The school will report any illegal activity conducted by a member of the school community to the relevant authority and will work with any victim involved to ensure they receive the support they require.

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Criminally racist material in UK (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- Promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Activities that might be classed as cyber-crime under the Computer Misuse Act: Gaining unauthorised access to school networks, data and files, through the use of computers/devices, creating or propagating computer viruses or other harmful files, etc…

6. *Dealing with unsuitable/inappropriate activities*

6.1 It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as follows

6.2 The school will take unsuitable/inappropriate behaviour online seriously, whether it has occurred in or outside of school.

6.3 All serious incidents are recorded and responded to by the online safety lead in coordination with the school's senior leadership and designated safeguarding team depending on the nature of the incident.

6.3.1 A serious incident could be but not limited to:

- incidents that have a significant detrimental impact on another person

- actions that bring the school or any member of the school community into disrupt
- any action that impacts the safety and security of the school

6.4 Staff must use their professional judgement when reporting any unsuitable/inappropriate activities but are encouraged to report if they are in any doubt. The school's child protection policy should be referred to if the incident is of a safeguarding nature.

6.5 Staff may choose to adapt their online safety curriculum in response to an incident, reteaching an aspect of online safety that is relevant to what has occurred.

6.6 If a child repeatedly breaks the 'Internet Safety Agreement', then alternative arrangements will be made so that the child does not have access to the internet or mobile device within school.

6.7 In the event that a child or young person accidentally accessing inappropriate material, the incident should be reported to the online safety lead immediately. If the incident has occurred in school, a full review of the filtering and monitoring systems will be conducted as a matter of urgency. If the incident has occurred at home, the child's parents/carers will be contacted so that the school can support them to mitigate the possibility of a repeat occurrence.

7. Social Media

7.1 It has, over the past decade, become more common place for primary age children to have social media and have a presence of networking sites. 40% of pupils aged 8-11 own a smartphone so we are teaching online safety to digitally active pupils. Social media has therefore become key strand of our teaching in upper KS2 as it is the most likely setting for our pupil's online safety teaching to be challenged.

7.2 The use of social networking sites within schools is only allowed in appropriately controlled situations and in support of legitimate curriculum activities – for example to teach the safe use of the internet.

7.3 Students must not access social networking sites for personal use via school information systems, school networks or using school equipment. The school's filtering system will obviously restrict these sites.

7.4 Social media platforms are often used as the vehicle to teach pupils about inappropriate behaviour and they are taught about the possible avenues to report concerns or abuse on social media platforms. Children are encouraged to consider the implications for misusing social media and oversharing or sharing inappropriate content.

7.5 The school regularly reviews the social media content that is taught to pupils to match the evolving popularity and developments of these networks.

7.6 Schools are vulnerable to material posted about them online and all staff should be made aware of the need to report this should they become aware of anything bringing the school's or it's wider communities reputation into disrepute.

7.7 The appropriate online conduct of all members of staff is outlined in the 'Acceptable Use of IT' Policy.

8. Mobile Devices (including Smartwatches)

8.1 Mobile phones and other personal devices are becoming more common place among children under 11 and as most devices have access to the internet, the school has adapted its practice.

8.2 Children may bring a mobile phone to school. This is primarily so that parents/carers can be contactable if the child walks home alone. However, these devices must be handed in to an adult on entering the classroom. The phone will then be returned at the end of the day.

8.3 The use of a mobile phone is strictly prohibited within school (this includes the playground). The school will confiscate any device being used and will only return it to a parent or carer.

8.4 The teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

8.5 Smart watches that have internet access or the ability to take and store photo/video content are not permitted in school apart from in exceptional circumstances.

9. Monitoring and updating the Online Safety Policy

9.1 Due to the ever-changing nature of digital technologies, it is best practice to review the Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

9.2 The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet filtering
- Internal monitoring data for network activity

Online Safety Curriculum Objectives

UPDATED September 2022

Taught Autumn Term 1 Taught Autumn Term 2

	Year 3	Year 4	Year 5	Year 6
1. How to evaluate what they see online	• **Know that not everything on the internet is true**, including people and misleading online content. (taught in PSHE too)	• **Attempt to distinguish between fact and fictional online content** (websites, fake emails, social media posts, YouTube videos, etc…) • Recognising the techniques used online to make believe something false is true/or mislead (misinformation)	• To understand that inaccurate and pervasive information exists online and we should be cynical of online content • **Recognise that not all information on the internet is accurate or unbiased** (advertising, persuasive/sticky design of online games, grooming)	• **To evaluate online content** (including social media) to **enable pupils to make judgements on its legitimacy** • Recognising the techniques used online to manipulate and mislead (misinformation, advertising, persuasive/sticky design of online games, grooming)
2. Online Behaviour & Relationships	• **To recognize that bullying can occur online** and describe appropriate ways to behave online • To understand that what it means to 'know someone' online and why this might be different from knowing someone offline (taught in PSHE lesson)	• Resolving online disagreements with friends, recognising cyberbullying and disengaging from unwanted contact online • **Identify where inappropriate behaviour may occur online** (i.e images, videos, text, chat…)	• Explore the motives behind negative online behaviour (anonymity, invisibility) • **Consider unacceptable online behaviour that is often passed off as social norms (banter)** • **Understand that online behaviour online can break the law**	• Explore the motives behind negative online behaviour (anonymity, invisibility, fake profiles) • Mob mentality intensifying online emotions • **Consider unacceptable online behaviour that is often passed off as social norms (banter)** • **Understand that online behaviour online can break the law**
3. Online Reputation and Dangers	• **To recognise that some people I may communicate with online may want to cause me harm** (taught in PSHE lesson) • **To identify information that I should not put online** and the reasons for this and how information I put online can last for a long time	• **To understand that what I share online can have positive and negative consequences**	• **Explore the positives and negatives of their actions onlin**e and ramifications to their own and others' reputation (digital footprint)	• Discuss the risks vs. benefits of sharing information online on their own and others' reputation • I **can recognise how judgements can be made about an individual based on the information they share online** • To understand the need for online privacy and how this can helps protect them from risks

				(with additional emphasis on online safety)
4. Identifying and Managing Online Risks	• Raise awareness of the dangers of giving personal information on the internet • **Understand what makes a strong password** and why these are essential to protect our online information	• **Look at the ways in which someone may put themselves at risk online by sharing personal information** • What to do if I think my password has been shared, lost or stolen	• **To understand the need for online privacy and how this can helps protect them from risks** • Know what the digital age of consent is (13)	• **To understand the need for online privacy and how this can helps protect them from risks** • Describe ways in which some online contents targets people to gain information illegally (scams, phishing…)
5. How and when to seek support	• **To know what action to take if they feel they may be in danger (trusted adults)** • I know how to support others who are having difficulties online	• **Identify a range of ways to report concerns about contact online** both in school and at home (including Childline)	• **Identify a range of ways to report and actions to respond to concerns online** including reporting and blocking users.	• **Recognise how negative online behaviour might change as I grow older** • To know how to capture evidence of content (screengrabs)