Online Safety Policy

Geoffrey Field Junior School

Written February 2025
Review February 2027

1. Rationale

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 Junior School 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. Aims

2.1 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

2.2 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, antisemitism, 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 scams

3. Legislation and Guidance

3.1 This policy is based on the Department for Education's (DfE's) 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

3.2 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.

4. Roles and Responsibilities

Governing Body

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

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

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

4.4 The governing board 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 review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

Head Teacher

4.5 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.

4.6 The Head Teacher, with support where appropriate, will ensure that the school's digital infrastructure is compliant with the 'Meeting Digital Standards in Schools' and that procedures for monitoring the use of technology are rigorous.

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

Designated Safeguarding Lead(s)

4.8 The DSL takes lead responsibility for online safety in school, supported by their deputies as set out in our child protection and safeguarding policy.

4.9 The DSLs

ICT Technician

4.10 The ICT technician is responsible for putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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.

4.11 The ICT technician will ensure the ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

4.12 The ICT technician will facilitate regular security checks and monitoring of the school's digital infrastructure. This includes assuring potentially dangerous sites are not accessible and, where possible, preventing the downloading of potentially dangerous files.

4.13 The ICT technician will liaise with the DSLs at the school to ensure monitoring systems are effective and incidents are tracked.

All Staff

4.14 Teaching and Support Staff are responsible for ensuring that they have a clear understanding of their role in implementing this policy.

4.15 All staff must work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy, including incidents of cyber-bullying.

4.16 If staff observe or suspect any misuse or concerns relating to any person's online behaviour of safety, these must be recorded and reported.

Parents & Carers

4.17 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 parent online safety workshops, literature on the school website and through policies.

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

Visitors & Volunteers

4.19 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.

5. Online Safety in the Curriculum

5.1 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.

5.2 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.

5.3 **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.

5.4 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

5.5 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

5.6 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.

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

5.8 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.

5.9 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.

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

6. Supporting Parents with online safety

6.1 Parents and carers play an essential role in educating their children about the importance of online safety and monitoring how their child interacts with the online world. 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.

6.2 The school 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

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

7. Dealing with illegal activities

7.1 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
- 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…

8. Dealing with unsuitable/inappropriate activities

8.1 Where the school deals with incidents that involve inappropriate rather than illegal misuse, it is important that they are dealt with as soon as possible in a proportionate manner.

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

8.3 All serious incidents are recorded and responded to in coordination with the school's senior leadership and designated safeguarding team depending on the nature of the incident. A serious incident could be but not limited to:

- incidents that have a significant detrimental impact on another person, including cyber-bullying.
- 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

8.4 Incidents of misuse will be dealt with in accordance with the school's behaviour policy and/or the school's child protection and safeguarding policy.

8.5 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. 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.

8.6 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.

8.7 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.

8.8 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.

9. Social Media

9.1 It has, over the past decade, become more commonplace for primary age children to have social media and have a presence of networking sites. 61% of pupils aged 8-11 own a smartphone so we are teaching online safety to digitally active pupils. Social media has therefore become a 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.

9.2 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.

9.3 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 restrict these sites.

9.4 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.

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

9.6 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 its wider communities reputation into disrepute.

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

10. Student Mobile Devices (including Smartwatches)

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

10.2 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.

10.3 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.

10.4 Smartwatches that have internet access or the ability to take and store photo/video content are not permitted in school and will be confiscated. Pupils are permitted to wear smartwatches that do not contain these features on the grounds that they are not a distraction during lesson.

10.5 Authorised staff members may examine 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
- Undermine the safe environment of the school or disrupt teaching
- Commit an offence

10.6 If inappropriate material is found on the device, the school's safeguarding team will 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.

10.7 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

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

11. Training

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

11.2 The DSL team 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.

12. Monitoring and updating the Online Safety Policy

12.1 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.

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

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

Online Safety Curriculum Objectives

UPDATED September 2025

	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** ● **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.	● **Identify a range of ways to report and actions to respond to concerns online** including how and when to report to CEOP. ● **Recognise how negative online behaviour might change as I grow older** ● To know how to capture evidence of content (screengrabs)

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)