

Online and E-Safety Policy



Approved by:	Julliette Young	Date: November 2023
Last reviewed on:	27/11/2023	
Next review due by:	Every 3 Years (Unless Guidance Changes)	

Contents

1. Aims.....	Error! Bookmark not defined.
2. Policy Scope	Error! Bookmark not defined.
3. Roles and responsibilities.....	Error! Bookmark not defined.
4. Educating pupils about online safety.....	Error! Bookmark not defined.
5. Support for Parents/Carers and carers with on-line safety.....	5
6. Training and engagement with staff	7
7. Reducing Online Risks	7
8. Filtering and Monitoring + Security and Management of Information Systems	8
10. Use of Personal Devices and Mobile Phones.....	10
10. How the school will respond to issues of misuse	Error! Bookmark not defined.
11. Training	Error! Bookmark not defined.
12. Monitoring arrangements.....	Error! Bookmark not defined.
13. Links with other policies.....	Error! Bookmark not defined.

Aims

This policy takes into account the DfE statutory guidance “[Keeping Children Safe in Education](#)” 2021 and [Early Years and Foundation Stage](#) 2017

The purpose of Bird in Bush Primary School’s online safety policy is to:

- Safeguard and protect all members of Bird in Bush’s community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

- Clarify the school’s position on the use of mobile phones in school
- Recognise our responsibilities in line with the new Keeping Children Safe in Education (KCSIE) 2023 guidance, particularly relating to school procedures and policies linked to internet filtering
- (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1161273/Keeping_children_safe_in_education_2023_-_statutory_guidance_for_schools_and_colleges.pdf)

There is an effective and whole school approach to online safety at Bird in Bush, which protects, educates and empower pupils and staff in their use of technology and establishes procedures for identifying, intervening in and escalating concerns. There are four main areas of risk within online safety:

- **Content** – being exposed to illegal, inappropriate or harmful content
- **Contact** – being subjected to harmful online interactions with other users. This can include peer on peer pressure, commercial advertising, adult or peer on peer grooming for the purposes of exploitation
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm – including online bullying and the making, sending and receiving of explicit images.
- **Commerce**- risks such as online gambling, phishing or other financial scams

There is an integrated whole school approach to teaching children about staying safe online and is reflected in the development of school policies and procedures, when planning the curriculum, teacher training and the support and training available for Parents/Carers and carers.

Policy Scope

Bird in Bush Primary School believes that:

- Online safety is an essential part of safeguarding and acknowledge their duty to ensure that all pupils and staff are protected from potential harm online.
- The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as ‘staff ‘in this policy) as well as pupils and Parents/Carers/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

Roles and Responsibilities

Executive Head Teacher – James Robinson

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

The Designated Safeguarding Lead DSL – Madeline Eastwood

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Executive Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Executive Head Teacher, computing lead and all staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- 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.

The ICT Manager – Paul Chin

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

The Governing Body

The governor who oversees online safety is Juliette Young

The Governing Body must ensure that:

- Pupils are taught about safeguarding including online safety.
- Teaching about safeguarding including online safeguarding is adapted for vulnerable pupils, victims or abuse and those pupils with SEND (as appropriate).
- Training requirements have regard to the Teacher's Standards which set out the expectation that all teachers manage behaviour (including pupils use of technology and social media) effectively to ensure a good and safe educational environment, where teachers have a clear understanding of all pupils needs.
- Staff training includes online safeguarding training and online safety and the requirement that children are taught about keeping themselves safe when on line and using social media and the internet safely and responsibly.

The Senior Leadership Team (SLT) will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a code of conduct and/or an Acceptable Usage Policy (AUP).
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training through regular staff meetings and as part of training

- Delegate to ICT co-ordinators the co-ordination of participation in local and national events to promote positive online behaviour, such as Safer Internet Day and the promotion of online safety to Parents/Carers, carers and the wider community
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the leadership team.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Executive Head Teacher of any concerns or queries regarding this policy.
- Ensure their child follows the terms of acceptable use of the school's ICT systems and internet.
- Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Educating pupils about online safety

Reviewing online safety

- At Bird in Bush we use independent technical support. They provide technical support in the development and implementation of appropriate online safety policies and procedures.
- They will implement appropriate security measures (*including password policies and encryption*) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools' filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the Executive Head Teacher and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the Executive Head Teacher, in accordance with the school's safeguarding procedures.

It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the school acceptable usage policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

Education and Engagement Approaches

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE and Computing programmes of study, covering use both at school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils to understand the acceptable usage in a way which suits their age and ability by:

- Displaying acceptable use posters.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Using support, such as external visitors, where appropriate, to complement and support the schools' internal online safety education approaches.

Support for Parents/Carers and carers with on-line safety

It is important for children and young people to stay both connected and safe online. Please see the link below for further advice.

<https://www.gov.uk/guidance/covid-19-staying-safe-online#Parents/Carers>

Make use of parental controls

If you have downloaded new apps or bought new devices like web cams or tablets, remember to adjust the privacy and security settings to suit you.

The Government has encouraged Internet Service Providers to help Parents/Carers easily filter content. [Switch on family friendly filters](#) to help prevent age-inappropriate content being accessed on devices in your home. Parental controls put you in control of what your child can see. Internet Matters has [step by step guides](#) on how to set these up.

If you are concerned or upset about something your child has seen online seek support from the online platform using the report function on the app or website - you can often find these in the 'help' section or 'settings' or seek support from other organisations and helplines. The UK Safer Internet Centre offers a service, [Report Harmful Content](#), which you can use if you are not satisfied with the result of a report.

Have a conversation with your child about staying safe online

Most children have a positive experience online, accessing educational resources and entertainment and connecting with friends and family. Spending time online can be very beneficial for children, particularly at the moment, but we recognise that many Parents/Carers may worry about online safety.

- **Reduce the risk:** The UK Council for Internet Safety has [guidance](#) on minimising children’s exposure to risks online. The UK Safer Internet Centre with Childnet International has specific guidance on [under 5s](#).
- **Talk to your child:** Childnet has [guidance](#) for Parents/Carers and carers to begin a conversation about online safety and [Ditch the Label](#) teacher resources that can be helpful for Parents/Carers to discuss cyberbullying and the government also has [helpful advice](#). Encourage your child to speak to you or a trusted adult if they come across content that makes them uncomfortable.
- **Help your child to think critically:** We can help protect our children by teaching them ‘critical thinking skills’ - a way of thinking that helps them spot potential harm and work out what to do. Critical thinking empowers children because they can take what they know and adapt it to new situations or to solve problems that may emerge. It helps them identify risks, which may protect them from different forms of threats and ultimately harm. Parent Zone’s [guide](#) and Childnet’s [advice and top tips](#) provides ways for Parents/Carers and carers to help their child develop these skills.
- **Stay safe and healthy:** You may be concerned about how long your children are using their devices. The government has published [guidance for Parents/Carers and carers](#) on supporting children and young people’s mental health and wellbeing during COVID-19.

The UK’s Chief Medical Officer has also provided [advice on screen time](#). Here are a few of the tips to help your children strike a balance:

- **Sleep matters:** Getting enough good quality sleep is very important. Leave phones outside the bedroom when it is bedtime.
- **Sharing sensibly:** Talk about sharing photos and information online and how photos and words are sometimes manipulated. Parents/Carers and carers should never assume that children are happy for their photos to be shared. For everyone – when in doubt, don’t upload!
- **Talking helps:** Talk with children about using screens and what they are watching. A change in behaviour can be a sign they are distressed – make sure they know they can always speak to you or another responsible adult if they feel uncomfortable with screen or social media use.
- **Keep moving:** Everyone should take a break after a couple of hours sitting or lying down using a screen. It’s good to get up and move about a bit. #sitlessmovemore
- **Family time together:** Screen-free meal times are a good idea – you can enjoy face-to-face conversation, with adults giving their full attention to children.
- **Use helpful phone features:** Some devices and platforms have special features – try using these features to keep track of how much time you (and with their permission, your children) spend looking at screens or on social media.

Pupils’ Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not condone the use of these sites by any pupils.
- Any concerns regarding pupils’ use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with Parents/Carers/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Where pupils are found to have profiles on sites and are under the specific age for joining those sites, the school will contact sites directly to inform them of the breach of their site policy.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords; to use social media sites which are appropriate for their age and abilities; and how to block and report unwanted communications and report concerns both within school and externally.

Official Use of Social Media

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use school provided email addresses to register for and manage any official school social media channels.
- Official social media sites are suitably protected and will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/Carers, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents/Carers and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff, with at least annual updates.
- This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils, including ensuring all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Reducing Online Risks

We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace therefore we will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

Filtering and Monitoring + Security and Management of Information Systems

Decision Making

- Bird in Bush Primary School has ensured that it has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The schools' decisions regarding filtering and monitoring have been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- The school uses London Grid for Learning (LGFL) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Executive Head Teacher and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/Carers/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies.

Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education.
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies
- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Head Teacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.

Social Media

Expectations

- The expectations' regarding safe and responsible use of social media apply to all members of the school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Bird in Bush Primary School are expected to engage in social media in a positive, safe and responsible manner, at all times. Staff are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- Concerns regarding the online conduct of any member of staff on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school code of conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Bird in Bush Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Head Teacher immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Use of Personal Devices and Mobile Phones

This policy recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and Parents/Carers/carers, but technologies need to be used safely and appropriately within school.

Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
- All members of staff are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour Policy.
- All members of staff are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child Protection policies.

Staff Use of Personal Devices and Mobile Phones

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Not use personal devices during teaching periods, unless permission has been given by the Executive Head Teacher, such as in emergency circumstances or for a medical need.
- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or Parents/Carers and carers unless calling out from a private number (+141).
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
 - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school policies.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Bird in Bush expects pupil's mobile phones to be handed into the school office at the beginning of the day and collected after school

- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policies.
- Pupils' mobile phones or devices may be searched by a member of Leadership Team with the consent of the pupil or a parent/ carer.
- Mobile phones and devices that have been confiscated will be released to Parents/Carers or carers.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

- Parents/Carers, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour and Child Protection.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Executive Head Teacher of any breaches of school policy.

Appendix 1: National Links and Resources

Useful Links for Educational Settings

Organisation	Link
Ask About Games	Askaboutgames provides a range of advice on how to stay safe online. It also features advice about finding balance during COVID-19.
CEOP	If you are worried about online sexual abuse or the way someone has been communicating with you online? Make a report to one of CEOP's Child Protection Advisors www.ceop.police.uk
GetSafe Online	www.getsafeonline.org
SafeToNet	SafeToNet is an app for Parents/Carers to help them safeguard their children from online risks like cyberbullying and sexting, whilst always respecting their child's rights to privacy. The SafeToNet Foundation is providing UK families with free for life access to the SafeToNet safeguarding solution during coronavirus.
BBC Own It App	The BBC Own It app helps children stop and think before they press the 'send' button.
Childnet	A tool kit to support Parents/Carers and carers of any age child to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support. www.childnet.com
Internet Matters	Internet Matters has created a #staysafestayhome hub. The hub has information about setting devices up safely, age appropriate conversations to have and resources to support families' wellbeing.
LGfL	Support for Parents/Carers and carers to keep their children safe online , including 6 top tips to keep primary aged children safe online.
Net-aware	Support for Parents/Carers and carers from NSPCC, providing a guide to social networks, apps and games .
Parent Info	Provides support and guidance for Parents/Carers from leading experts and organisations.
Thinkuknow	Provides advice from the National Crime Agency (NCA) to stay safe online. To help families manage during this time, the NCA has launched #OnlineSafetyAtHome , a set of fun, engaging activities based on Thinkuknow cartoons, films, games, and advice articles.
UK Council for Internet Safety	Education for a Connect World . A framework to equip children and young people for digital life.
NSPCC:	The NSPCC is here to support Parents/Carers talk to their children about online safety. From setting up parental controls to advice on sexting, online games and video apps, they can help parent to understand the risks and keep your child safe. www.nspcc.org.uk/onlinesafety
ChildLine	www.childline.org.uk
UK Safer Internet Centre	The UK Safer Internet Centre, provides online safety tips, advice and resources to help children and young people stay safe online. www.saferinternet.org.uk