Carleton Green Primary School

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- *Headteacher*
- *Deputy Headteacher*
- *Computing Coordinator*
- *PSHE Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Governing Body on:*	
The implementation of this online safety policy will be monitored by the:	*SLT*
Monitoring will take place at regular intervals:	*Written: May 2020* *Reviewed: December 2023* Revisit: September 2024
The *Governing Body* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*S. McGrath (DSL)* *S. Clark (Deputy DSL)*

The school will monitor the impact of the policy using:

- *Logs of reported incidents on CPOMS*
- Pupil, parent and staff voice

Scope of the Policy

This policy applies to all members of the *school* (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy along with The 2022 Keeping Children Safe in Education.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school. It will take into account the National Curriculum Computing Programme of Study along.

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

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* receiving 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: A Walker*
- *regular monitoring of Online Safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors / Board / committee / meeting*

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including Online Safety) of members of the school community**
- **The Headteacher and (at least) another member of the Senior Leadership Team 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.**
- *The Headteacher and Senior Leaders are responsible for ensuring that the Online 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.*
- *The Headteacher 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *Monthly filter check by Headteacher and Business Manager.*

Online Safety Coordinator:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The *Co-ordinator for ICT / Computing* is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required Online Safety technical requirements and any *Local Authority / other relevant body* Online Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / ICT systems / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Principal / Senior Leader; Online Safety Coordinator*

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of Online Safety matters in addition to Safeguarding of the current *school* Online Safety policy and practices.**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher* for investigation / action / sanction**
- **all digital communications with students / 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
- students / pupils understand and follow the Online Safety and acceptable use policies
- students / 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, mobile devices, cameras etc 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 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*

Child Protection / Safeguarding Designated Person

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 adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- Keep Children Safe in Education: content, contact, conduct and commerce.

Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way to keep children safe online. The *school* will take every opportunity to help parents understand these issues *through parents' evenings, newsletters, letters, website and information about national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice including UK Safer Internet Childnet and to follow guidelines on the appropriate use of:*

- digital and video images taken at school events
- access to parents' sections of the website / blog
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / 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 and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned Online Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**

- *Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that 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.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*
- *Remote Learning, if needed will be accessed through the class home learning pages on the school website.*

Education – parents / carers

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 / regulation of the children's on-line 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.

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

- *Curriculum activities*
- *Letters, newsletters, website,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications*

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and Online Safety*
- *Online Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school / academy website will provide Online Safety information for the wider community*
  Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training – Staff / Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify Online Safety as a training need within the performance management process.*
- **All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.**

- *The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems** • **Servers, wireless systems and cabling must be securely located and physical access restricted.**
- **There will be monthly filter check by Headteacher and Business Manager.**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **The headteacher / LA officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** • *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.* • *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers

to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.** • In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases
  protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

	Staff & other adults						
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	✓					✓	
Use of mobile phones in lessons				✓			
Use of mobile phones in social time	✓			✓			
Taking photos on mobile devices		✓					✓
Use of other mobile devices eg tablets, gaming devices							✓
Use of personal email addresses in school, or on school network			✓	✓			
Use of school email for personal emails				✓			
Use of messaging apps				✓			
Use of social media			✓	✓			
Use of blogs (the school blogsite)	✓				✓		

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

When using communication technologies the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully (please see our behaviour policy), discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
comments that contain or relate to:	**promotion of any kind of discrimination**				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media				X		

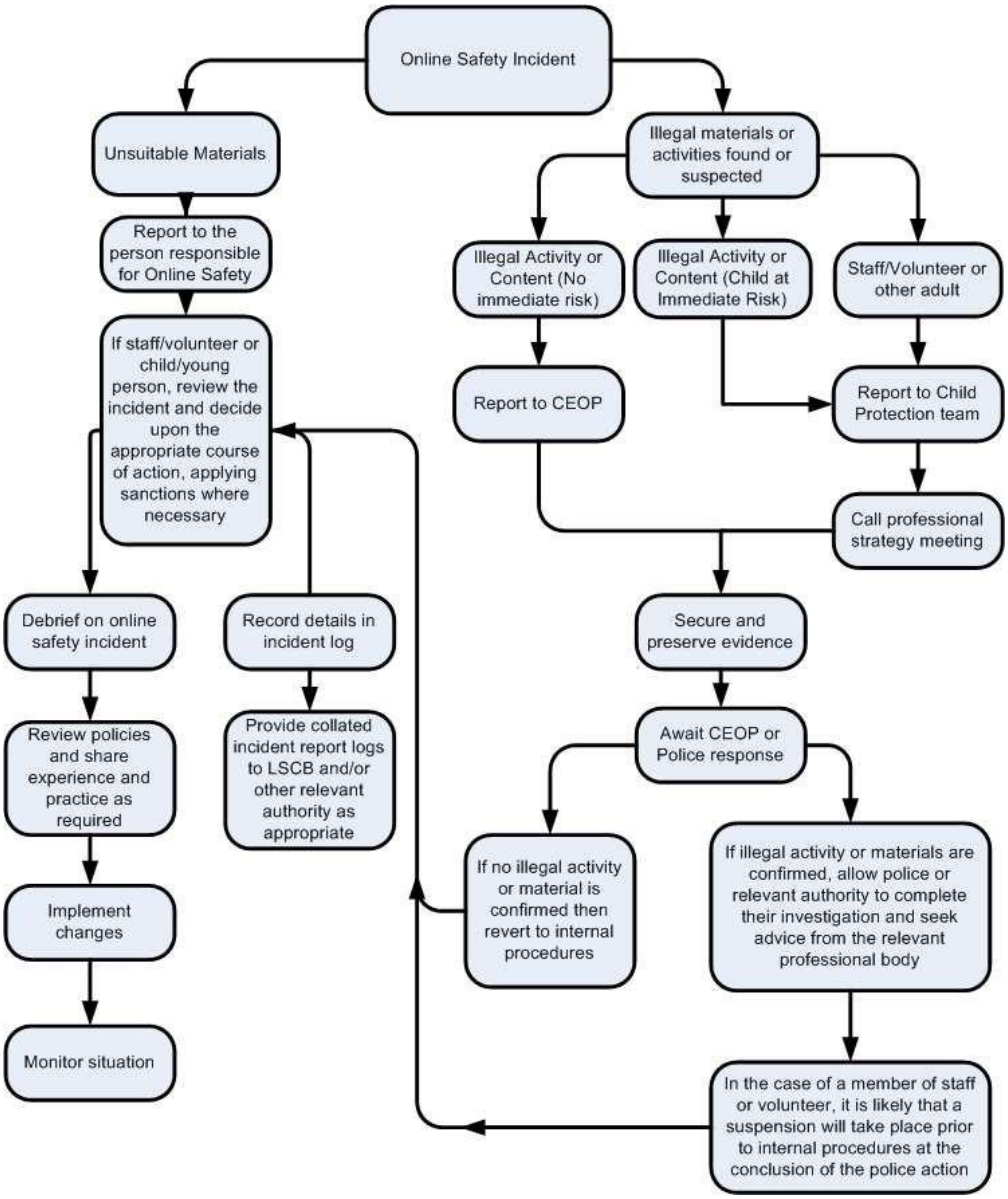
Use of messaging apps				X	
Use of video broadcasting eg Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act • criminally racist material
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school / academy 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 / disciplinary procedures as follows:

Students / Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X

Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

APPENDICES

Carleton Green Community Primary School
Arundel Drive, Carleton, Lancashire. FY6 7TF
Tel: (01253) 891228 Fax: (01253) 896227
Email: head@carletongreen.lancs.sch.uk

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not engage with or make friends with parents of children at school on Facebook or other Social Networking Sites.

6. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

7. I will respect copyright and intellectual property rights.

8. I will ensure that all electronic communications with children and other adults are appropriate.

9. I will not use the school system(s) for personal use during working hours.

10. I will not install any hardware or software without the prior permission of the network manager

11. I will ensure that personal data (including data held on systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

12. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will

not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

13. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

14. I will report any known misuses of technology, including the unacceptable behaviours of others.

15. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

16. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

17. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

18. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

19. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

20. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.

21. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..

Date ……..

Full Name ……..……(PRINT)

Please return your completed form to Mrs Davis

Carleton Green Community Primary School

Arundel Drive, Carleton, Lancashire. FY6 7TF
Tel: (01253) 891228 Fax: (01253) 896227
Email: head@carletongreen.lancs.sch.uk

ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

Signature

We have discussed this Acceptable Use Policy and …… [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at Carleton Green Primary School.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) …… …… Class …… Date……

Carleton Green Community Primary School

Arundel Drive, Carleton, Lancashire. FY6 7TF
Tel: (01253) 891228 Fax: (01253) 896227
Email: head@carletongreen.lancs.sch.uk

September 2021

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website, or in school displays, including digital photo frames.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third parties who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely,

Mrs McGrath
Headteacher

Carleton Green Community Primary School

Arundel Drive, Carleton, Lancashire. FY6 7TF
Tel: (01253) 891228 Fax: (01253) 896227
Email: head@carletongreen.lancs.sch.uk

Image Consent Form

Name of the child's parent/carer:…….

Name of child:……

Year group:.....

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (one for each child) should be returned to school as soon as possible. (Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?	Yes	No
2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events?		
3. May we use your child's image in printed school publications and for digital display purposes within school?		
4. May we use your child's image on our school's online publications e.g. website / blog?		
5. May we record your child on video?		
6. May we allow your child to appear in the media as part of school's involvement in an event?		

I have read and understand the conditions of use attached to this form

Parent/Carer's signature:
……

Name (PRINT): …… Date: ……

Arundel Drive, Carleton, Lancashire. FY6 7TF
Tel: (01253) 891228 Fax: (01253) 896227 Email:
head@carletongreen.lancs.sch.uk

Conditions of Use

1. This form is valid for this academic year 2021-2022

2. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.

3. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.

4. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

5. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.

6. 3rd Parties may include other children's parents or relatives e.g. attending a school production.

7. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.

8. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.

2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.