On-Line Safety Policy

Resilience
Respect
Responsibility

Name of School:	North Clifton Primary School
Reviewed by Governors:	October 2022
Responsibility of:	Governors
Next Review Date:	October 2024

Introduction and Values Statement

At North Clifton Primary School we all know the experiences a child has during the formative years of their life have such an impact on the kind of person they will develop into and become in the future. Such a lot of this important time is spent at school so it is essential that we work in partnership with parents so that we can make a positive difference and create a strong foundation that can be built upon as children continue to grow, develop and flourish.

North Clifton Primary School is centred around the 3 R Values

Resilience

Respect

Responsibility

Our North Clifton Primary Values underpins the curriculum that we deliver ensuring that all our pupils become aspirant, independent and confident life-long learners, who have empathy towards one another and are prepared to take risks in their learning. We believe children learn best when they feel happy, secure, confident and valued, irrespective of their ability or disability, social background, culture or gender. As a school, we complement the government's idea of British/Human Values. Pupils are helped to understand the importance of democracy, the rule of the law, freedom of speech and respect for others through the curriculum and extra curricula activities. They are also encouraged to understand the importance of taking responsibility for their own behaviour and thinking about the choices they make both in school and online.

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience. We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We take pride in sharing our 3 R Values with parents and carers. As a consequence of our values, we aim to provide all our pupils with a safe, caring and friendly environment in order to allow them to improve their life chances and help them maximise their potential.

We expect all pupils to act safely and feel safe in school, including understanding the issues relating to all forms of bullying, and that they have the confidence to seek support from the school should they feel that they or others are unsafe. We want parents/carers to feel confident that their children are safe and cared for in school and that incidents and problems, should they arise, are dealt with promptly and well.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremist's groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism as well as regular discussions with all classes on the importance of being aware of whom they may be in contact with online.

All school personnel are aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead. At North Clifton Primary School, we are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent Duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

The school is aware of its legal obligations including the Equalities Act 2010. We are aware of our role within the local community: supporting parents/carers and working with other agencies (where appropriate) outside the school.

Policy Development

This policy was formulated in consultation with the whole school community with input from pupils, staff, parents/carers and governors.

- Children and young people – (school council),
- Members of staff- (for example though agenda items at staff meetings and consultation documents),
- Governors – (discussions at governor meetings, training and consultation documents),
- Parents/carers – (for example parents will be encouraged to contribute by taking part in written consultations, parent meetings and producing a shorter parent's guide).

This policy is available:

- Online on the school website,
- From the school office.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body	**October 2022**
The implementation of this online safety policy will be monitored by the:	**Online Safety Coordinator/ DSL – Karen Clifton**
Monitoring will take place at regular intervals:	**Termly**
Governing Body will receive a report on the implementation of the online safety policy annually:	
The online safety policy will be reviewed every 2 years. The next anticipated review date will be:	**October 2024**
Should serious online safety incidents take place, the following external persons/agencies should be informed:	**LA Safeguarding Officer, LADO, Police**

The school will monitor the impact of the policy using:

- Logs of reported incidents,
- Monitoring logs of internet activity (including sites visited)/filtering,
- Internal monitoring data for network activity,
- Surveys/questionnaires of,
    - Pupils,
    - parents/carers,
    - staff.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers 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 online-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. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

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.

Roles and Responsibilities

As a school, the staff at North Clifton have a responsibility to implement this policy.

This includes:

The Governors:

Governors are responsible for the approval of the North Clifton Primary online safety policy and for reviewing the effectiveness of the policy.

The Head Teacher:

Has overall responsibility for the policy and its implementation and liaising with the governing body, parents/carers, LA and outside agencies and appointing an Online Safety coordinator who will have general responsibility for handling the implementation of this policy.

The Designated Safeguarding Lead in our school is Anne Batley. Safeguarding is the responsibility of all. However all staff, parents and pupils need to be aware of who to report to and how to report any safeguarding concerns.

The Online Safety Coordinator in our school is:- Karen Clifton

Their responsibilities are: -

- Takes day to day responsibility for online safety issues and has a leading role in establishing, reviewing and implementing 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 school IT staff,
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Manages the reporting and recording of bullying incidents both in school and online,
- Coordinating strategies for preventing online incidents.

The nominated Governor with the responsibility for E Safety (Behaviour) is - Andrew Jackson

Definition of Bullying

The repetitive, intentional hurting of one person or group by another person or group, where the relationship involves an imbalance of power. Bullying can be physical, verbal or psychological. It can happen face-to-face or through cyberspace.

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices,
- They have read, understood and signed the staff acceptable use policy (AUP),
- They report any suspected misuse or problem to the head teacher/ online safety lead for investigation/action,
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems,
- Online safety issues are embedded in all aspects of the curriculum and other activities,
- Pupils understand and follow the online safety policy and acceptable use policies,
- Pupils have a good understanding of research skills and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons 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

Designated Safeguarding Lead

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,
- Online-bullying.

Pupils

- Are responsible for using the school's digital technology systems in accordance with the pupil acceptable use agreement,
- 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 online-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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, emails, website, social media and information about national/local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events,
- Access to parents' sections of the website/learning platform and on-line pupil records.

Policy Statements

Education – Pupils

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/digital literacy 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.

In planning their online safety curriculum school may refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- The RSHE policy and PSHE Progression document

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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making,
- N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet,
- 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 children visit.

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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities,
- Letters, newsletters, web site, Learning Platform,
- Parents/carers meetings,
- High profile events/campaigns e.g. Safer Internet Day,
- Reference to the relevant web sites/publications e.g.
    - www.swgfl.org.uk
    - www.saferinternet.org.uk
    - http://www.childnet.com/parents-and-carers

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 planned 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.

National College, Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff (https://boost.swgfl.org.uk/)

- 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,
- It is expected that some staff will identify online safety as a training need within the performance management process,
- The Online Safety Lead will receive regular updates 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.

Training – Governors

- Governors should take part in online safety training sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising

the school's wireless network. The device then has access to the wider internet that may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, anti-bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	Limited	Limited
Internet only	Yes	Yes	Yes	NA	Yes	Yes
Network access	Yes	Yes	Yes	No	No	No

Use of digital and video images: There is a separate Child Images Policy

Data Protection – there is a separate data protection policy.

Communications

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 (e.g. by remote access),
- Users must immediately report to the nominated person – in accordance with the school 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 pupils or parents/carers (email, social media, chat, blogs, VLE etc) 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,
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate

communications and be reminded of the need to communicate appropriately when using digital technologies,
- 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, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school 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:

- Ensuring that personal information is not published,
- Training is provided including: 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,
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders,
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff,
- A code of behaviour for users of the accounts, including:
    - Systems for reporting and dealing with abuse and misuse,
    - Understanding of how incidents may be dealt with under school disciplinary procedure.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school,
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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	
	Promotion of any kind of discrimination				x	
	Threatening behaviour, including promotion of physical violence or mental harm				x	
	Promotion of extremism or terrorism				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	

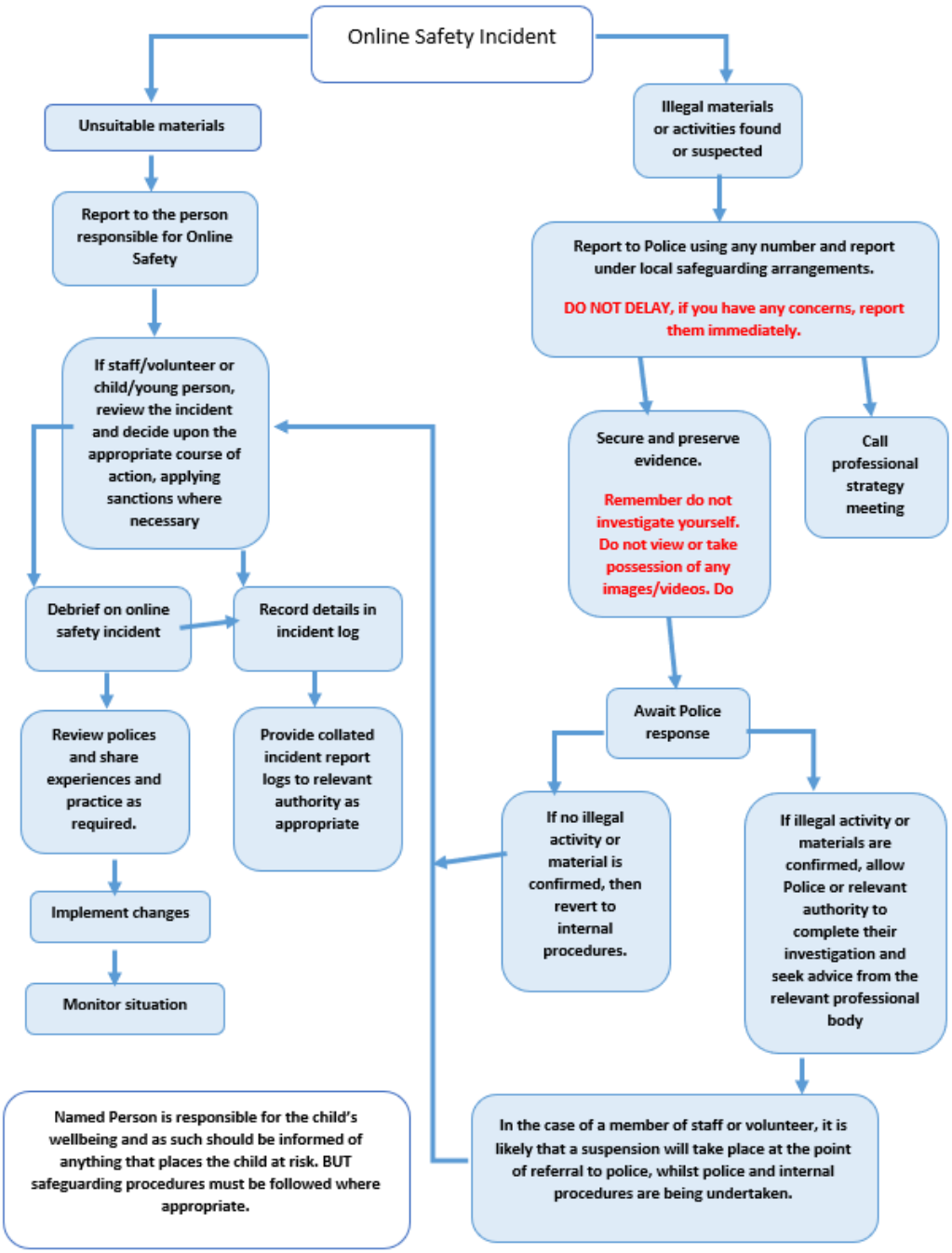
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					x
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				x	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				x	
Using school systems to run a private business				x	
Infringing copyright				x	
On-line gaming (educational)		x			
On-line gaming (non-educational)				x	
On-line gambling / shopping/ commerce				x	
File sharing		x			
Use of social media / messaging apps / video broadcasting e.g. 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 and appendix) 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 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 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 pupils 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,
    - 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,
    - promotion of terrorism or extremism,
    - offences under the Computer Misuse Act (see User Actions chart above),
    - 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 and possibly the police and demonstrate that visits to these sites were carried out for safeguarding 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 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:

	Actions/Sanctions								
Pupils Incidents	Refer to class teacher	Refer to DSL/SLT	Refer to Head Teacher	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 e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		x	x	x					
Unauthorised use of non-educational sites during lessons	x	x							
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x	x	x						
Unauthorised/inappropriate use of social media/ messaging apps/personal email	x	x	x						
Unauthorised downloading or uploading of files	x	x							
Allowing others to access school network by sharing username and passwords	x	x				x			
Attempting to access or accessing the school network, using another pupil's account	x	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				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 filtering system				x	x	x			
Accidentally accessing offensive or pornographic material and failing to report the incident				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	x	x		

	Actions/Sanctions							
Staff Incidents	Refer to line manager	Refer to Head Teacher	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				
Inappropriate personal use of the internet/social media/personal email		x	x					
Unauthorised downloading or uploading of files		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					
Careless use of personal data e.g. holding or transferring data in an insecure manner		x	x					
Deliberate actions to breach data protection or network security rules		x	x	x				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x	x				
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with 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	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	x					
Deliberately accessing or trying to access offensive or pornographic material		x	x	x				
Breaching copyright or licensing regulations	x	x						
Continued infringements of the above, following previous warnings or sanctions		x	x	x				

Appendix

Appendix A

During Covid 19 times some of our expectations for the use of mobile phones in the classroom and around children has changed as we learn to manage in isolation away from other staff. As a result, we have put together an appendix of ways to work during these unprecedented times.

SLT recognise the importance of interaction and communication between staff to avoid movement around the building and cross contamination of bubbles. Staff should only use mobile phones when it is necessary and appropriate to do so.

Staff may also be asked to communicate with families and children as part of their safeguarding role.

When using mobile phones in school staff are still expected to

- Make calls which are limited to discussion about general wellbeing, not about lesson plans or work to be completed,
- All 'welfare calls' made by designated safeguarding leads to vulnerable children or by other staff should be logged on the vulnerable children list,
- Staff should not be encouraged to use their own personal phones or devices. Online calling facilities are safer for students and staff and are accessible. i.e. Through the use of Teams
- If there is no alternative to using personal phones, safety measures are put in place. Staff should dial 141 before dialling the pupil's number: this will withhold the caller's number, thereby protecting and safeguarding the adult's personal number. Staff should delete numbers from their phones after use,
- Staff should try to pre-arrange calls with parents/carers to find an appropriate time, as families are juggling many commitments,
- Staff should ask to speak to a parent at the start of the call, giving their name and explaining why they are calling, and should end the call by speaking to the parent again. No personal information should be disclosed during the call,
- Families not responding to staff for more than a week need to be followed up according to the Covid safeguarding protocol,
- This protocol may revert to the original policy once the Covid situation returns to 'normal'.

Pupil Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications,
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone will steal it,
- I will be aware of "stranger danger", when I am communicating on-line,
- I will not disclose or share personal information about myself or others when on-line. (This could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material, messages, or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and*:*

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission,
- I will immediately report any damage or faults involving equipment or software, however this may have happened,
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings,
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work,
- Where work is protected by copyright, I will not try to download copies (including music and videos),
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the schoo*l* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the North Clifton Primary School systems and devices (both in and out of school)

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Pupil Acceptable Use Policy Agreement

– for younger pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

Signed (parent): .....

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Pupil Name: .....

As the parent/carer of the above pupils, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....

Date: .....

Remote Learning/ Teams Home/ School Agreement