	<h1>Online Safety Policy</h1>	<p>Resilience Respect Responsibility</p>
<p>This policy was reviewed by the Governing Body: September 2024</p>	<p>Next review: September 2025</p>	
<p>Chair of Governors: Karen Grundy Head Teacher: Ilona Sanderson</p>	<p>Strategic Lead: Ilona Sanderson</p>	

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, our values incorporate Fundamental British 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)
- Governors – (discussions at governor meetings, training),
- Parents/carers – (for example during parent meetings and information on our website).

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	September 2024
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator/ DSL – Ilona Sanderson
Monitoring will take place at regular intervals:	Termly
The online safety policy will be reviewed annually:	September 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, LADO, Police

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors including filtering and monitoring systems
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Roles and Responsibilities

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

This includes:

The Governors:

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

Our Governing body will ensure they maintain oversight of the Online Safety Policy alongside our main child protection policy, and the arrangements put in place to ensure appropriate filtering and monitoring on school devices and school network. The appropriateness of any filtering and monitoring systems will in part be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2024 paragraphs 145 to 146.

This will include:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet the school/ colleges safeguarding need.
- review and discuss the standards with the leadership team, IT staff and service providers to ensure the school/college meets the standard published by the Department for Education filtering and monitoring standards.

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

The governing board will also make sure all staff receive regular online safety updates (via emails and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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

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

Details of the school's designated safeguarding lead (DSL) and deputy DSL are set out in our child protection and safeguarding policy.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Online Safety Coordinator in our school is: Ilona Sanderson

Their responsibilities are: -

- Maintains the on-line safety policy which informs of the filtering and monitoring arrangements on ICT devices and networks to keep children safe and is reflected in this Child Protection Policy including awareness of the vulnerabilities when accessing to mobile phone networks. (See KCSiE 2024 Paragraphs 12,102,123 and 133 to 146). It also address statutory filtering and monitoring standards and use of mobile and smart technology and is reviewed regularly to take into account any new threats.
- Takes day to day responsibility for online safety issues and has a leading role in establishing, reviewing and implementing school online safety policies/ documents,
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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.

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
 - What are the issues? – [UK Safer Internet Centre](#)
 - Hot topics – [Childnet](#)
 - Parent resource sheet – [Childnet](#)

Visitors and members of the community

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

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.

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

Education – Pupils

All schools have to teach:

[Relationships education and health education](#) in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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 World 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

The school will 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.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see below, page 13, for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

North Clifton Primary recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

North Clifton Primary will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use..

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

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 policies 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 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: Parents are requested to only take photographs of their own children at events and not to share any images on-line that contain pictures of other children.

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
- 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	

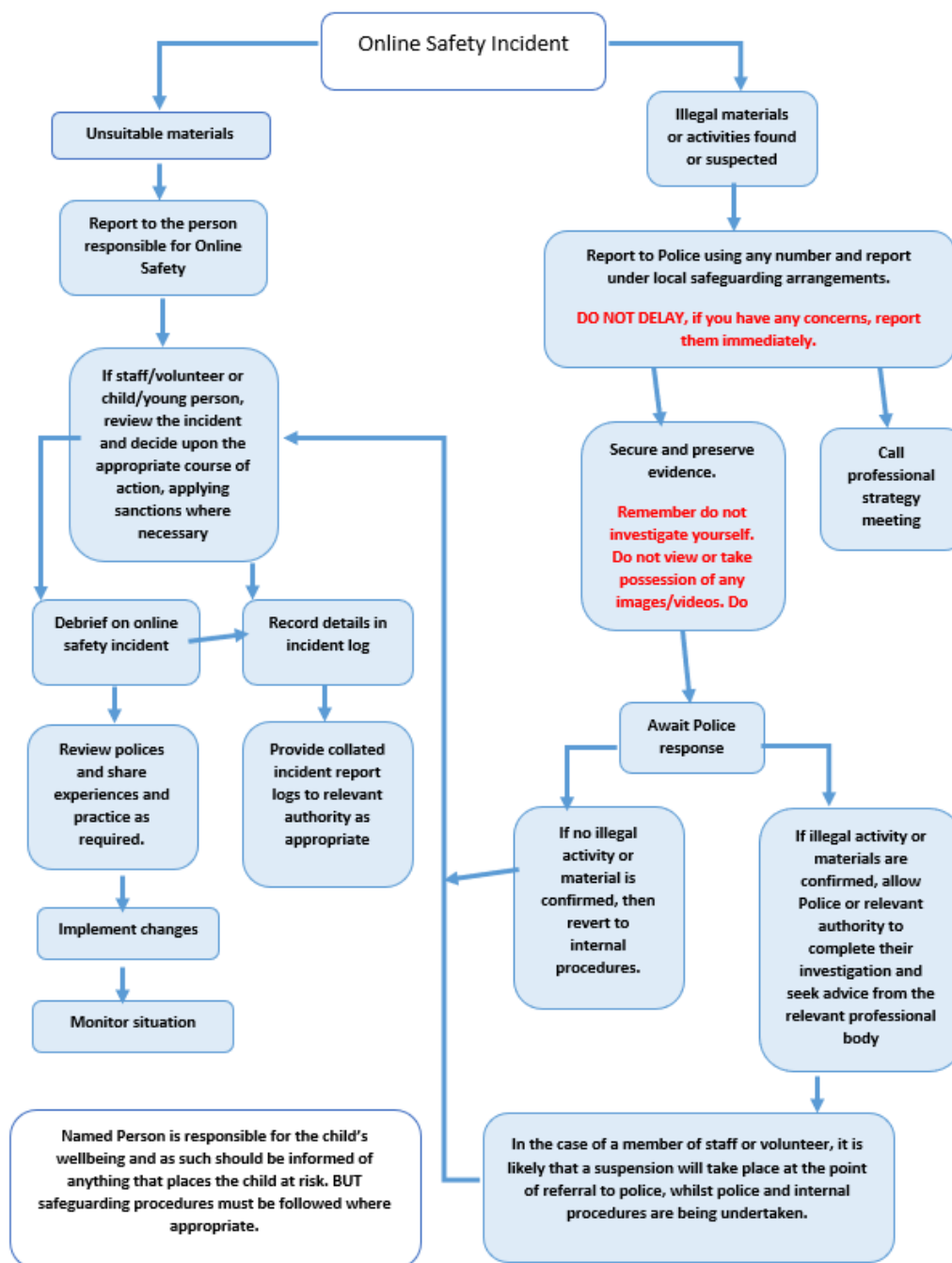
<p>Activities that might be classed as cyber-crime under the Computer Misuse Act:</p> <ul style="list-style-type: none"> • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing 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								
	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
Pupils Incidents									
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							
	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
Staff Incidents								
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 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

NORTH CLIFTON PRIMARY: ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will:	
<ul style="list-style-type: none">• Ask a teacher or adult if I can do so before using them• Only use websites that a teacher or adult has told me or allowed me to use• Tell my teacher immediately if:<ul style="list-style-type: none">○ I select a website by mistake○ I receive messages from people I don't know○ I find anything that may upset or harm me or my friends• Use school computers for school work only• Be kind to others and not upset or be rude to them• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly• Only use the username and password I have been given• Try my hardest to remember my username and password• Never share my password with anyone, including my friends• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer• Save my work on the school network• Check with my teacher before I print anything• Log off or shut down a computer when I have finished using it	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (pupil):	Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

NORTH CLIFTON PRIMARY: ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy.	
When I use the school's ICT systems (like computers) and get onto the internet in school I will:	
<ul style="list-style-type: none">• Always use the school's ICT systems and the internet responsibly and for educational purposes only• Only use them when a teacher is present, or with a teacher's permission• Keep my usernames and passwords safe and not share these with others• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer• Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others• Always log off or shut down a computer when I've finished working on it	
I will not:	
<ul style="list-style-type: none">• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity• Open any attachments in emails, or follow any links in emails, without first checking with a teacher• Use any inappropriate language when communicating online, including in emails• Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate• Log in to the school's network using someone else's details• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision	
If I bring a personal mobile phone or other personal electronic device into school:	
<ul style="list-style-type: none">• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (pupil):	Date:
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	Date:


Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:	
<ul style="list-style-type: none">• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)• Use them in any way that could harm the school's reputation• Access social networking sites or chat rooms• Use any improper language when communicating online, including in emails or other messaging services• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network• Share my password with others or log in to the school's network using someone else's details• Take photographs of pupils without checking with teachers first• Share confidential information about the school, its pupils or staff, or other members of the community• Access, modify or share data I'm not authorised to access, modify or share• Promote private businesses, unless that business is directly related to the school	
<p>I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.</p> <p>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.</p> <p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.</p> <p>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.</p> <p>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.</p>	
Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

 ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident