Northstead Community Primary School

Seek to Learn

Northstead Community Primary School

Online Safety Policy

Document Status			
Date of Next Review	June 2023	**Member of staff responsible**	Miss L Roberts Mrs S Wilson Mr R Gay
Success Criteria for review completion		**Senior Member of staff responsible**	Mr S. Hopper
Date of Policy Creation	**Adopted NYCC written model**	**Governor responsible**	Mrs J Laybourn
Date of Policy Adoption by Governing Body:			**Signed** J. Laybourn
Method of Communication:	Website and through staff training		

Contents:

1. Introduction

At Northstead Community Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for children and play an important role in their everyday lives.

Whilst Northstead Community Primary School recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and staff.

The school is committed to providing a safe learning and teaching environment for all children and staff, and has implemented important controls to prevent any harmful risks.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 2018
- General Data Protection Regulation 2018
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

This policy also has regard to the following statutory and non-statutory guidance:

- Keeping Children Safe in Education (DfE, 2022)
- Teaching online safety in school (DfE, 2019)
- Education for a Connected World (UK Council for Internet Safety, 2020)
- RSE & Health Education (DfE, 2019)

2. Aims

- To actively provide and promote opportunities for developing children's skills to develop safe online behaviour.
- To ensure that staff are able to identify and respond to all potential forms of online safety incidents.
- To ensure that children are aware of how and to whom online safety incidents should be reported and understand that all online safety concerns will be dealt with sensitively and effectively.
- To ensure that parents/carers are aware of online safety issues and know whom to contact if they are worried about online safety issues.

3. Keeping children safe online (KCSiE 2022)

The school understands that using the internet is not only a skill that children need to learn but an important tool in enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore an entitlement for all children. However, there are a number of controls required in order to minimise harmful risks.

When accessing the internet, individuals are vulnerable to a number of risks which may be physically and emotionally harmful. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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

4. School Website

The contact details on the website show the school address, e-mail and telephone number. Staff or children's personal information will not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photographs that include children will be selected carefully and will not enable individual children to be clearly identified without the prior consent of the child's parent/carer.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents/carers will be obtained when the child begins school before photographs of children are published on the school website.

5. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school.

Governors

The governing body will ensure online safety is a running and interrelated theme throughout the implementation of the whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Headteacher and Senior Leaders

- The Headteacher has overall responsibility for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinators.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinators and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring (Smoothwall) and will support those in school who carry out the internal online safety monitoring role.
- When necessary, the Senior Leadership Team will receive monitoring reports from the Online Safety Co-ordinators.

- The Headteacher and Deputy Headteachers (as designated child protection persons) will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see section 14).

Online safety Coordinators

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (CPOMS)
- Provides training and advice for staff.
- Liaises with school IT technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (CPOMS).
- Meets annually with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant Governors meetings.
- Reports to the Senior Leadership Team

All online safety incidents will be reported immediately to the Designated Safeguarding Lead (S Wilson) or the Deputy Designated Safeguarding Lead (L Roberts) using CPOMS to decide the most appropriate way of dealing with them and whether the incidents are child protection issues, in which case they will be dealt with in accordance with the school's child protection procedures.

Technical staff

The Computing Co-ordinator and Technician are responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the online safety technical requirements outlined in the relevant Local Authority Online safety Policy and guidance.
- That he/she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the Online safety Co-ordinator/Headteacher/Deputy Headteacher/Assistant Headteachers for investigation/action/sanction.
- That monitoring software/systems are reviewed regularly, implemented and updated as agreed in school policies.

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 school Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or problem to the Online safety Co-ordinators/Headteacher/Deputy Headteacher using CPOMS for investigation/action/sanction.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Children understand and follow the school Online Safety and Acceptable Use Policy.
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, tablets, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

- In lessons where internet use is pre-planned children 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 person for Child Protection

The Designated and Deputy Designated Child Protection officers will be trained in and keep up to date with developments in online safety issues, remaining aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Potential radicalisation

Children

- Are responsible for using the school IT systems in accordance with the Child Acceptable Use Policy which is provided at the start of their time at the school. Parents/carers may sign on behalf of their child/ren.

- Will be taught when appropriate to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of tablets, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will therefore take every opportunity to help parents understand these issues through termly internet safety and mobile phone awareness sessions, newsletters, letters, the school website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- Attending an internet safety and mobile phone awareness session prior to allowing their child to bring a mobile to school.
- Endorsing (by signature) the Child Acceptable Use Policy and Parent Acceptable Use Policy.
- Accessing the school website.

6. Technical – infrastructure / equipment, filtering and monitoring

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

- School IT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school IT systems such as servers, wireless systems

- The "master/administrator" passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place. The school will never allow one user to have sole administrator access.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security, although when working in pairs in class it may be necessary for children to share their partner's log-on.
- The school maintains and supports the managed filtering service (Smoothwall) provided by the Local Authority.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged in the Online Safety Record and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately
- Requests from staff for sites to be removed from the filtered list will be considered by the Computing Co-ordinator and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- School IT technical staff use Smoothwall to monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy
- An appropriate system is in place (CPOMS) for users to report any actual/potential online safety incident to the Online Safety Co-ordinator.
- Appropriate security measures are in place (for example CDC) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attacks which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system – guest log-ons are available.
- The school infrastructure and individual workstations are protected by up to date virus software. Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

7. Online safety Education and Training

Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education

of children in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety education will be provided at Northstead Community Primary School in the following ways:

- A planned online safety programme will be provided as part of our Computing Scheme of Work and/or through PSHE/other lessons. It will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and learning activities.
- Children will 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
- Children will be helped to understand the need for the child AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet when appropriate.
- Rules for use of IT systems/internet will be posted in all rooms.
- Staff will act as good role models in their use of IT, the internet and mobile devices.

Staff

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.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
- The Online Safety Coordinator will receive regular updates through attendance at Local Authority/other information/training sessions and by reviewing guidance documents released by the LA and others.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Online Safety Coordinator will provide advice/guidance/training to individuals as required.

Governors

Governors will take part in online safety training/awareness sessions. This may be offered in a number of ways:

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

8. Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of IT across the curriculum.

- In lessons where internet use is pre-planned, children will be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet e.g. using search engines, staff will be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Computing Co-ordinator/Headteacher can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Requests for website release should be made on an appropriate request proforma (see Appendix 1).
- Children will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- When appropriate children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism

9. Use of Digital and Video images - Photographic, Video (see policy for use of photos and images)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school

will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment - the personal equipment of staff should not be used for such purposes.
- Children and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and Class Dojo
- Care will be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere, that include children, will be selected carefully.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of children are published on the school website (consent form signed by parents/carers at the start of the year)

10. Cyber Bullying

Opportunities for children to bully or to be bullied via technology, such as e-mail, texts or a wide range of social media sites are becoming more frequent nationally. As such, teaching children about appropriate behaviours when using technology provides a vital grounding for future use

- The school's Anti-Bullying Policy will address Cyber-bullying (see Anti-Bullying Policy).
- Children, parents/carers, staff and governors will all be made aware of the consequences of cyber-bullying.
- Children and their parents/carers will be made aware of a child's rights and responsibilities in their use of new technologies and what the sanctions are for misuse.
- Parents/carers will be provided with an opportunity to find out more about cyber-bullying through information and/or sessions for parents/carers.
- The school will take all reasonable precautions to prevent cyber-bullying whilst children are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor North Yorkshire County Council can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with children in preventing cyber-bullying by:

- Understanding and talking about cyber-bullying e.g. inappropriate use of e-mail, text messages etc;
- Keeping existing policies and practices up to date with new technologies;
- Promoting the positive use of technology;

Records of any incidents of cyber-bullying will be kept on CPOMS and will be used to help to monitor the effectiveness of the school's prevention activities.

11. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table, taken from 'Online Safety Guidance for Schools and Settings in North Yorkshire' (January 2021), shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Pupils			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	☐					☐		
Mobile phones used in lessons				☐				☐
Use of mobile phones in social time	☐ As outlined in the mobile phone policy	☐ As outlined in the mobile phone policy						☐
Staff should only contact a pupil on a school issued mobile phone				☐				
Taking photographs/film on personal mobile devices / digital camera				☐				☐
Taking photographs/film on school mobile devices / digital camera for school purposes only	☐						☐	
Parent / carer taking photos of a school event on their own device	☐ Not permitted to upload onto social media if other children visible							
Use of personal tablets/ laptops ipads etc in school		☐						☐
Use of school owned tablets/ laptops/ ipads in school but not for personal use	☐				☐			
Use of school owned tablets/ laptops/ ipads out of school but not for personal use	☐ (within the AUP)				☐ (within the AUP)			

Only using school provided encrypted storage devices		□				□			
Use of school email for personal emails					□				□
Social use of chat rooms/facilities					□				□
Use of social network sites in school				□					□
Use of educational blogs		□						□	

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 can be monitored. Staff and children should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications can be monitored.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and children or parents/carers (Class Dojo 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 public chat/social networking programmes must not be used for these communications
- Children will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

12. Data Protection

Everyone responsible for recording, processing, transferring and using personal data will follow the 'data protection principles' as outlined in the Data Protection Act 2018 which states that everyone's personal data must be:

- Fairly, lawfully and transparently processed
- Used for specific, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Staff must ensure that they:

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

When personal data is stored on any portable computer system, USB stick or any other removable media, at least one of the following must apply:

- The data must be encrypted and password protected.
- The device must be password protected (some memory sticks/cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, once it has been transferred or its use is complete.

13. Unsuitable/inappropriate/illegal 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 IT 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					☐
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☐
Adult material that potentially breaches the Obscene Publications Act in the UK					☐
Criminally racist material in the UK					☐
Pornography					☐
Promotion of any kind of discrimination				☐	
Any Hate Crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					☐
Promotion of any kind of extremist activity					☐
Promotion of racial or religious hatred					☐
Accessing any extremist materials online (e.g Far Right Extremism)				☐	
Threatening behaviour, including promotion of physical violence or mental harm					☐
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 e.g discussing school issues on social media				☐	
Using school systems to run a private business				☐	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				☐	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☐	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				☐	
Creating or propagating computer viruses or other harmful files				☐	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☐	
On-line gaming (educational)		☐			
On-line gaming (non- educational)				☐	
On-line gambling				☐	
On-line shopping / commerce			☐		
File sharing			☐		
Use of social networking sites			☐		
Downloading video broadcasting e.g. Youtube for educational purposes	☐				
Uploading to video broadcast e.g. Youtube			☐		

14. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

This table, taken from 'Online Safety Guidance for Schools and Settings in North Yorkshire' (January 2021), should be consulted and actions followed in line with the table, in particular the sections on reporting the incident to the police and the preservation of evidence.

Incidents involving members of staff	Refer to the Headteacher *See below	Refer to technical support staff for action re filtering, security etc	Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	□	□	□
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	□		□
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	□	□	□
Unauthorised downloading or uploading of files	□	□	□
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.	□	□	□
Careless use of personal data e.g. holding or transferring data in an insecure manner	□		□
Deliberate actions to breach data protection or network security rules	□	□	□
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	□	□	□

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	□	□	□
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	□	□	□
Actions which could compromise the staff member's / governors professional standing	□		□
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	□		□
Using proxy sites or other means to subvert the school's filtering system	□	□	□
Deliberately accessing or trying to access offensive or pornographic material	□	□	□
Breaching copyright or licensing regulations	□	□	□
Continued infringements of the above, following previous warnings or sanctions	□		□

*In event of breaches of policy by the Headteacher, refer to the Chair of Governors.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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.

Incidents involving pupils – either in school or out of school – it could be a concern raised by a friend/ parent	Teacher to use school behaviour policy to deal with	Refer to Senior member of staff	Refer to pupil behaviour and refer to external agencies if required	Refer to technical support staff for action re security/filtering etc
A concern raised by a pupil/ teacher / friend/ parent (carer). A pupil need positive support – Signs of grooming Signs of peer on peer abuse / grooming / power domination Signs of radicalisation Signs of CSE Signs of cyberbullying		☐	☐	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).		☐	☐	☐
Unauthorised use of non-educational sites during lessons	☐			☐
Unauthorised use of mobile phone/ digital camera/ other handheld device.	☐			
Unauthorised use of social networking/ instant messaging/ personal email and online gaming	☐	☐		☐
Unauthorised downloading or uploading of files		☐		☐
Allowing others to access school network by sharing username and passwords		☐		☐
Attempting to access or accessing the school network, using another student's account		☐		☐
Attempting to access or accessing the school network, using the account of a member of staff		☐		☐
Corrupting or destroying the data of other users		☐		☐
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		☐		☐
Continued infringements of the above, following previous warnings or sanctions		☐	☐	☐
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		☐		☐
Using proxy sites or other means to subvert the school's filtering system		☐		☐
Accidentally accessing offensive or pornographic material and failing to report the incident		☐		☐

15. Social networking and personal publishing

[redacted]

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Children are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and Northstead Community Primary School as a whole.
- Staff are not permitted to communicate with children over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about Northstead Community Primary School which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours.

- **Mobile devices and hand-held computers (See Mobile Phone Policy)**

- Staff are permitted to use hand-held computers which have been provided by Northstead Community Primary School, though internet access will be monitored for any inappropriate use by the Online Safety Coordinator when using these on the school premises.
- Personal devices must not be used to take images or videos of children or staff.
- The use of mobile phones by staff, parents and volunteers is detailed in the Mobile Phone Police and Acceptable Use Agreements.

Appendix 1

Northstead Community Primary School

Requests for website release

Website release being requested	
Member of staff requesting the release	

Northstead Community Primary School

Seek to Learn

Please give a description below of how this website will be used in the classroom and how this will have a positive impact on the children's learning.

Signed: (member of staff requesting the website release) _____ Date: _____

Signed: (Online-Safety Co-ordinator) _____ Date: _____

Request accepted/rejected?

Date: _____ Signed: _____