NORTHSIDE Primary School

Online Safety Policy

Last review: March 2021
Ratified: March 2021
Review: Sept 2021

Rationale
The online world has many positive and exciting opportunities which can support pupils' learning. At Northside we must ensure that we give all stakeholders the skills and knowledge to deal with the challenges and risks that are involved with accessing online materials; this policy outlines our approach and the procedures we have in place.

This policy is based on the following legislation;

- Keeping Children Safe in Education (DfE)
- 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
- 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.

Northside Values

RESPECT	to value our needs, beliefs and each other
PRIDE	to have confidence in our abilities and celebrate success
INCLUSION	to work together with families and our diverse community to become life-long learners
CHALLENGE	to have high expectations of ourselves so we achieve our best
CREATIVITY	to creatively express our feelings and ideas
RESILIENCE	to develop life skills so we fulfil our potential

UN Rights of the Child:
Article 13 - Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.
Article 17 - Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

Key Principles

- Set out the expectations of all the Northside community with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language and misogynist language and scenarios), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- exposure to websites connected to radicalisation and extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- grooming for radicalisation
- online-bullying in all forms,
- cyber-bullying is like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Contents

Section 1: Overview - The Acceptable Use of the Internet and related Technologies

a. Context
b. The Technologies
c. Whole school approach to safe use in Computing
d. Roles and responsibilities
e. Communications
f. How will complaints regarding online safety be handled

a. Context

A good school 'integrates issues about safety and safeguarding into the curriculum so that pupils have a strong understanding of how to keep themselves safe. The school is pro-active in building on collaborative working with other key agencies to reduce the risk of harm to pupils.'

The Working Together to Safeguard Children sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.
This policy is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

b. The Technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include, for example:

- The Internet
- E-mail
- Instant messaging
- Blogs (an online interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites e.g. Youtube
- Chat Rooms
- Gaming Sites e.g. Club Penguin, Minecraft
- Gaming consoles with online gaming e.g Xbox Live, Playstation Network
- Music download sites e.g. Itunes, Amazon
- Mobile phones with camera and video functionality

- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Smart TVs

c. Whole School Approach to the safe use in Computing
Creating a safe Computing learning environment includes three main elements at Northside Primary School:
● An effective range of technological tools;
● Policies and procedures, with clear roles and responsibilities;
● A comprehensive Online Safety education programme for pupils and staff

d. Roles and Responsibilities
Online Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy is monitored. The responsibility for online safety has been designated to the senior leadership team and the Designated Safeguarding Lead.

Our school Online Safety Leaders are *Liz Longworth* (Headteacher) and *Aikaterini Rapti* (Computer Science Leader)
Our IT technician is *Nayif Abdo* (Turn IT On)
Our Designated Safeguarding Lead is *Jonathan Harper*
Our Safeguarding Governor is *Lorna Nsoatable*
Our Online Safety Governor is *Lorna Nsoatable*

Our Online Safety Leaders and Designated Safeguarding Lead ensure they keep up to date with online safety issues and guidance through liaison with the Local Authority Online Safety Officer, Turn IT On support and through organisations such as The Child Exploitation and Online Protection (CEOP). The school's Designated Safeguarding Lead ensure the Senior Leadership Team and Governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms, ensuring pupils are given clear objectives for Internet use, taught what is acceptable and follow the school online safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with Northside's Policy including:
- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- GDPR regulations;
- Cyberbullying procedures;
- Their role in providing Online Safety education for pupils.

Staff are reminded / updated about Online Safety matters as part of the September INSET. New staff are given the Online Safety Policy during induction.

Online Safety is an integral part of the Computing Curriculum, under Digital Literacy. Pupils need to know how to control and minimise online risks and how to report a problem.

Northside Primary School makes every effort to engage with parents over online safety matters and parents/guardians/carers are asked to sign and return an AUP form when their child starts at the school and again at the start of KS2. In addition, the school website features an Online Safety section in the 'Parents' Area (https://northside-primary-school.secure-primarysite.net/online-safety/)

e. Communication

How is the policy introduced to pupils?

- Pupils are always reminded of how to keep themselves online before accessing internet. This is embedded as part any ICT lesson.
- Online Safety training is included in the Computing Scheme of Work (Switched on Computing) covering both school and home use.
- Online safety is taught in all year groups, covering age-appropriate issues. Useful online safety programmes include
    - Barnet and LGfL online safety and Framework for EYFS-Y6 (https://www.lgfl.net/online-safety/default.aspx)
    - Think U Know (www.thinkuknow.co.uk/)
    - Grid Club (www.gridclub.com)
    - CEOP (https://ceop.police.uk/

How is the policy discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies. Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their Computing use in school, they should discuss this with their line manager to avoid any possible misunderstanding. Computing use is widespread and all staff including administration, caretaker, governors and helpers are included in appropriate awareness raising and training. Induction of new staff includes information about the Online Safety Policy. There are clear procedures for reporting issues.

How are parents kept informed?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.

- A partnership approach with parents is encouraged including raising issues with Parent Forum. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Our website is also regularly updated with information about online safety. As well new information shared in our weekly newsletter when applicable.

f) How are complaints regarding online safety handled?

At Northside Primary School will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither Northside Primary School nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview with class teacher, a member of the Senior Leadership Team or Headteacher;
- informing parents or carers;
- fixed term exclusion;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including work];
- referral to Barnet LA / Police.

Any complaint will be dealt with using our Complaint Policy procedure. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and Barnet LA child protection procedures.

Section 2: Managing the Internet Safely

At Northside Primary School the following safety procedure are put in place;

● Pupils are always supervised by an adult when using the internet

●The filtered broadband connectivity is through the LGfL and so connects to the 'private' National Education Network;

●Additional user-level URL filtering is in-place using a secure service.

● Anti-virus software Sophos / other and network are set-up so pupils cannot download executable files such as .exe / .com / .vbs etc.;

● Caching is used as part of the network set-up;

● The Turn It On technician works closely with LGfL services and keeps up to date with their policies;

● The Turn It On technician ensures that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;

● Individual log-ins are used to log-on and access Microsoft Teams

● All staff only send personal data over the Internet using the school email or by uploading to Microsoft Teams (through which data is secured by log-ins and 'sharing' folders/files with only those concerned) Communication of sensitive information to the LA is via USO-FX. Personal level data should not be taken off-site unless it is on an encrypted device.

● Pupils only publish within appropriately secure learning environments such as on the class blog on our website or via Microsoft Teams and this is only shared with classmates/class teacher and webpages are only published internally.

Use of the Internet

At Northside Primary School:

- We supervise pupils' use at all times
- We use the pan-London LGfL Atomwide NetSweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached], including any 'comments sections' [e.g. when accessing youtube videos], to check for suitability. Alternatively, use sites accessed from managed 'safe' environments such as the LGfL content site, Purple Mash, BBC Bitesize etc;
- We plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Are vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Staff and students report any failure of the filtering systems directly to the Turn It On technician, who reports to LA / LGfL where necessary;
- We block all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- We have blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;
- Pupils (and their parent/carer) from EYFS, Key Stage 1 and 2, must individually sign an acceptable use policy form which is fully explained and used as part of the teaching programme; this ensures parents provide consent for pupils to use the Internet
- We use closed / simulated environments for e-mail for pupils;
- All staff and volunteers to sign an acceptable use agreement form and keeps a copy on file;
- Any incident of any bullying or inappropriate behaviour is recorded on CPOMs
- Any material we suspect is illegal is immediately reported to the appropriate authorities – the Police and Barnet LA

Education and Training

At Northside Primary School we:

- Foster a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher and click the REPORT button.
- Ensure pupils and staff know what to do if there is a cyber-bullying incident;
- Ensure all pupils know how to report abuse;
- Have a clear, progressive online safety education programme throughout all Key Stages, built on Barnet LA, LGfL and Switched on Computing online safety curriculum framework (EYFS-Primary). Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;

    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / websites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite at all times; keeping personal information private;
    - to understand how photographs can be inappropriate, manipulated and how web content can attract the wrong sort of attention;
    - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; online gaming / gambling;
- Ensure staff know how to encrypt data where the sensitivity requires and that they understand data protection and general computing security issues linked to their role and responsibilities;
- Update staff and/or makes training available to staff on online safety
- Runs a programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on website;
    - demonstrations, practical sessions held at school;
    - distribution of 'Think U Know' for parents materials
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

Section 3: Managing Email

At Northside Primary School:

- Only anonymous or group e-mail addresses e.g. office@northside.barnetmail.net are used for communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we may contact the police.
- Accounts are managed effectively, with up to date account details of users.

- Staff members who have left the school are removed from the school email system.
- Messages relating to or in support of illegal activities may be reported to the authorities.
- Spam, phishing and virus attachment can make e-mail dangerous. We use filtering software to stop unsuitable mail. Suspected failure of software to filter potential spam, phishing emails or viruses to be reported to the Turn IT On technician.

Pupils:

- We use Microsoft Teams for email with pupils.
- Pupils are introduced to and use e-mail as part of the Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail i.e.
    - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted;

Staff:

- Staff only use barnetmail or Microsoft Teams for confidential information;
- Ensure that e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.

Section 4: Use of Digital Images

At Northside Primary School;

- The Senior Leadership Team and School Secretary take editorial responsibility to ensure that the website content is accurate, quality of presentation is maintained and complies with copyright;
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;

- Photographs published on the web do not have full names attached (except Staff within the 'About Our School' section).
- Uploading of information on the school's network is shared between different staff members according to their responsibilities
- We gain parental / carer permission for use of digital photographs or video involving their child as part of GDPR consent form when their child joins the school. Parents have the right to refuse/limit permission for their child's work and/or image to be published/ Permissions are listed on the 'permission for photos or images latest update' spreadsheet, updated by the Admin assistant and distributed regularly to staff;
- Digital images / video of pupils are stored in staff on the shared drive or their school laptop and images should be deleted at the end of the year – unless an item is specifically kept for a key school publication, evidence for professional development or educational purposes within school;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to our website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- We only include first names in the school newsletter when images accompany the article. Children featured in newsletter images are checked against the 'permission for photos or images latest update' spreadsheet' before submission to ensure we have parental permission to publish as newsletters now are accessible to the world via the new website;
- Staff sign the Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their online safety education programme;

Social networking (other than our school website):

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.

- Schools should be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
- It is not acceptable for a member of staff to have links with a current or past pupil via a social networking site.

Section 5: Managing Equipment

- To ensure the network is used safely, we will:
- Ensure staff read and sign that they have understood Online Policy. Following this, they are set-up with email access and can be given an individual Microsoft Teams log-in username and password;
- Give pupils' individual log for Microsoft Teams
- Make it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Make clear that no one should log-on as another individual user – if two people log on at the same time this may corrupt personal files and profiles;
- Have set-up the network with a shared work area for each class
- Require all staff users to always log off when they have finished working or are leaving the computer unattended;
- Request that staff and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and projectors when they are not being used e.g. between lessons, over lunch break.
- Have set-up the network so that users cannot download executable files / programs;
- Have blocked access to music download or shopping sites – except those approved for educational purposes;
- Scanned all mobile equipment with anti-virus before it is connected to the network;
- Make clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus software maintained up-to-date
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities. Laptops are signed for and this is record is kept in their personnel file. All laptops are listed on the inventory and assigned to the relevant member of staff or area within the school. Staff should inform the Admin Assistant if they wish to reallocate equipment;
- Maintain equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / Technician; equipment installed and checked by approved Suppliers / LA electrical engineers;
- Not allow any outside Agencies to access our network remotely except where there is a e.g. technical support or MIS support through LA systems;
- Use the LGfL USO-FX / DCSF secure s2s website for all CTF files sent to other schools, and the Perspective Lite system within the LA
- Ensure that all pupil level data or personal data sent over the Internet is encrypted or sent within the approved secure system in our LA ;

- Follow LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Review the school ICT systems regularly with regard to security.

Section 6: Electronic Devices – Searching and Deletion

The changing face of information technologies and ever increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher will need to authorise those staff who are allowed to carry out searches.
The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: the Headteacher, the Designated Safeguarding Lead and, in their absence, the person left in charge of the school.

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Pupils encouraged not to bring mobile phones or other personal electronic devices into school. However lone travellers may need the security of a mobile phone and these will be given to the class teacher in the morning and locked away until home time.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is 'prohibited'(as defined in Section 550AA of the Education Act 1996)

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item. The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched and there must be a witness.

Extent of the search:
The person conducting the search may not require the pupil to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the pupil has or appears to have control – this includes desks and bags.
A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school code of conduct).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Sharing nudes and semi-nudes: how to respond to an incident
In the latest advice for schools and colleges (UKCCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices. The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.
This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention.
Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. Your setting's child protection policy should outline codes of practice to be followed.

- Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- Do not share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL

Section 7: How will infringements be handled

Pupils
Any pupil infringements will be dealt with initially by the class teacher and referred to a member of the Senior Leadership team or the Headteacher if the offence is repeated, is regarded as bullying or is of a serious nature e.g. deliberate mis-use of software/equipment. Parents may be informed and sanctions imposed e.g. loss of a privilege. All incidents will be recorded on CPOMs.

Staff
In the case of an alleged infringement, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. All sanctions are to be considered within the school's disciplinary procedures.

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, extremist, radical, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all Computing equipment by an outside agency, such as the school's managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in school.
- Identify the precise details of the material.

Schools are likely to involve external support agencies as part of these investigations e.g. a technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography
In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number 0808 100 00 40 at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html
http://www.iwf.org.uk

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within Online Safety / Acceptable Use Policy. All staff will be required to sign Online Safety Policy acceptance form and to sign indicating that they have read this policy
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate acceptable use form;
- Northside's Online Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

Section 8: Roles and Responsibilities

Role of the Governors

- Governors need to have an overview understanding of online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on online Safety and are updated at least annually on policy developments.
- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Quality of Education Committee.

Role of the Senior Leadership Team

- Developing, owning and promoting the online safety vision to all stakeholder of the school.
- Supporting the development of an online safety culture
- Making appropriate resources available to support the development of an online safety culture
- Receiving and regularly reviewing online safety incident recorded on CPOMs
- Supporting the leader in the appropriate escalation of any incidents
- Taking ultimate responsibility for online safety incidents

Role of the Designated Safeguarding Lead

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, IT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

Role of the Computer Science Leader

- Developing an online safety culture and acting as a named point of contact for all online safety issues
- Promoting online safety to all groups of the Northside community
- Ensuring that online safety is embedded within CPD for staff and across the curriculum
- Developing an understanding of the relevant legislation
- Liaising with the LA and other agencies as appropriate
- Reviewing and updating online safety policies and practice on a regular basis.

Role of the Teaching Team

- Contributing to the development of online safety policies
- Reading and signing staff Acceptable Use Agreements and adhering to them
- Taking responsibility for the security of systems and data, which includes ensuring that all sensitive information is stored on an encrypted storage device
- Having an awareness of online safety issues, including cyber-bullying, and how they relate to the children in their care
- Actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be, how to report cyber-bullying whether they are a victim or witness to the incidents
- Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives
- Embedding online safety education in curriculum delivery wherever possible including the DfE Relationships Education and Health Education guidance 2020 of;
  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
    - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- Identifying individuals of concern and taking appropriate action
- Knowing when and how to escalate online safety issues
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school
- Taking personal responsibility for their professional development in this area

Role of Pupils

- Responsible for using the school digital technology systems in accordance with the Pupil's Acceptable Use Policy

- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understand the importance of adopting good online safey 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

Role of Parents and Carers

- Contributing to the development of online safety policies
- Reading Acceptable Use Agreements, encouraging their children to adhere to them, and adhering to them themselves where appropriate
- Using the school website and other network resources safely and appropriately
- Discussing online safety issues with their children, supporting Northside Primary School in its online safety approaches and reinforcing their behaviours at home
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Modelling appropriate uses of new and emerging technologies

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Parent factsheet - Childnet International

Section 9: Using New Technology - Hints and Tips for adults working with children and young people

Read this, it might be helpful …

Social Networking hints and tips

Social networking sites are brilliant ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, **have a range of privacy settings**. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs etc., can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post embarrassing material.
- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.
- Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.
- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.
- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.
- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.
- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.
- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.
- You do not have to be friends with someone to be tagged in their photo album.
- If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.
- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.
- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.
- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour!
- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

Wider Internet hints and tips

- Never tell anyone your password.
- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any work found in a dictionary.
- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.

- Be careful when form filling online…., do you know who the data is for? Only answer 'required 'questions, do not just give out information because you have been asked for it.

- Never verify banking details online.

- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.

- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.

- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.

- Popup adverts are often a nuisance. Close them carefully as a 'close' button will often lead you to more advertising as the 'X' might be a graphic.

- If you get an email or popup offer that seems too good to be true it probably is! Watch out for online cons – it is like online door step selling.

- If someone sets things up for you at home, make sure you change your password immediately. Someone with your username and password could impersonate you.

- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.

- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.

- Use legal sites for downloading music, films etc., such as iTunes.

- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.

- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.

- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.

- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.

- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.

- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.

- Your school or work laptop (or other equipment) should not be used by friends and family.

If you work with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, London MLE 'room', or interactive whiteboard resource etc.

- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.

- Use child-friendly search engines with younger pupils. Older young people will use a variety of search engines at home; you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.

- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.

- Watch YouTube (or any) videos before you use them in the classroom.

- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.

- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.

- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.

- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.

- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device.

- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.

- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the NEN, LGfL or other sites your school / LA has advised you of. You cannot show DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.

Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.

- If you get an email from someone or a company that you have never head of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.

- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.

- Webmail is useful but insecure, and your email address is easily passed on.

- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.

- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.

- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.

- Don't give out private email addresses to students and pupils.

Phone hints and tips

- Don't give out your mobile number or home number to students or pupils.

- If you have a Bluetooth phone do you know if Bluetooth is turned on or off? If it is on is there a password? Open un-passworded Bluetooth means anyone else with Bluetooth in range can read the content of your phone or device.

- Many hand held games consoles have wireless and Bluetooth and can be used to make contact from 'stranger' devices within range.

Section 10: Microsoft Teams Home Leaning Agreement.

The school will be using Microsoft Teams to deliver home learning activities and live lessons (Teams Meetings). Every child will have their own user logon and password to get into their school Teams account.
Having your own Teams account comes with certain rights, responsibilities and conditions of use. These conditions will be listed below:

Rights:

- ✓ You have the right to expect lessons to be set up and delivered by your teachers.
- ✓ You have the right to have work planned, set up and delivered to you on Teams.
- ✓ You have the right to expect structured activities with dates and times when work should be done.
- ✓ You have the right to ask questions and seek help when needed (during normal school hours).
- ✓ You have the right to expect your work to be looked at by your teacher and for your teacher to provide feedback on some pieces of your work.

Responsibilities:

- ✓ The same high standards of behaviour, which are shown in class lessons, are expected to be followed in online lessons. Your online class is not to be used as an area for general chat (just as your class lessons are not).
- ✓ You have the responsibility to join live lessons on time and to be dressed in your uniform
- ✓ You will sign into your Microsoft Teams account every morning for registration and check the "Posts" section to see when your live lessons are happening and to see what work has been set for you.
- ✓ You will not write anything in the Teams Class "Posts" area unless you are asked to do so by your teacher.
- ✓ You will not use the "Chat" area of live lessons (Teams Meetings) unless you are asked to by your teacher.
- ✓ Any comments you do add must be respectful and given in the same manner you would if you were in class in school.
- ✓ You must not screenshot, record video or record sound in meetings – you do not have the permission of your teacher of classmates to do this. Your teacher may record the lesson and share it afterwards for any children who were unable to attend – this will be done through Microsoft Teams.

Consequences:

- ✓ If you follow the things asked of you above, you can expect to have a good online learning experience.
- ✓ If you misuse your school Microsoft Teams account (such as: disrupting lessons, sharing screenshots or video, speaking disrespectfully, using the Chat and Post sections for anything other than school use) your account may be deactivated. Alternative arrangements will be made, such as: parents will be sent recordings of live lessons and paper copies of work will need to be collected from school.

NORTHSIDE Primary School

Acceptable Use Policy for Staff and Governors Policy

Last review: September 2020
Ratified: 24.5.17
Review: September 2021

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download or save sensitive or personal data onto a personal device, I will store this data on the school server and or school devices.
- I will ensure that I work in a secure environment where my screen is not visible to others when working on sensitive or personal data.
- I will always log out when I finish working.
- I will report any data breaches to the SLT/ Data Protection Officer as soon as possible.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any confidential school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. I will not use my own phone to communicate with parents without prior approval of the Headteacher except in an emergency and I will withhold my number.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the ICT leader.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive) that does not have up-to-date anti-virus software to the network / Internet and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras, tablets, laptops or other equipment for taking

and transferring images of pupils or staff without permission and will not store images without consent of the data subjects.

- I will not use a mobile phone or other photographing equipment of my own to take any pictures of children.
- I will ensure that I secure ICT hardware using appropriate safety measures:
- My class laptop will be secured at all times
- Laptops/netbooks used by children will be locked away in a secure cupboard or the ICT suite at the end of each school day.
- Other items of ICT hardware e.g. cameras, will be secured in lockable cupboards when not in use.
- I will use cloud systems in accordance with School advice.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".
- I will only use school hardware for business purposes and personal purposes in a responsible way which minimises the risk of any data breaches. I understand that I will be subject to disciplinary procedures in line with our staff code of conduct and online safety policy should any breaches occur.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the Headteacher.

Within Social Networking:

- I will not contact pupils using social media or any other means not authorised by the school
- If any of my online activity affects students, staff or the wider community I understand that this could lead to disciplinary action
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that I cannot publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- I will not use Social Networking sites for the promotion of personal financial interests, commercial ventures or personal campaigns
- I will not breach any of the school's policies

- I will not discuss or advise any matters relating to school events or matters, staff or pupils without prior permission from the Head Teacher
- I will not identify myself as a representative of the school
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy for Staff and Governors Policy Sept 2020

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I agree to abide by all the points above.

I wish to have an email account and be able to use the school's ICT resources and systems.

Signature _____ Date:

Full Name _____ (printed)

Role within the school _____

NORTHSIDE Primary School

Online Safety Agreement 2020-21
KS1

My name is _____

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **KNOW** people online aren't always who they say	
5. I don't keep **SECRETS** just because someone asks me to	
6. I don't change **CLOTHES** in front of a camera	
7. I am **RESPONSIBLE** so never share private information	
8. I am **KIND** and polite to everyone	
9. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
10. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	

My trusted adults are:

_____ **at school**

_____ **at home**

NORTHSIDE Primary School
Online Safety Agreement 2020-21
KS2

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I can't go to school because of coronavirus*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first tim

14. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult: at school

Outside school, my trusted adults are_____

Signed: _____ Date: _____

NORTHSIDE Primary School

Parents Acceptable Use Policy 2020-21

Background

We ask all children, young people and adults involved in the life of the School to sign an Acceptable Use* Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
Your child has also signed an AUP in school.
We tell your children that **they should not behave any differently when they are out of school or using their own device or home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

What am I agreeing to?

1. I understand that the School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this

would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.
8. **I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.**
9. **If my child has online tuition for catchup after lockdown or in general, I will undertake necessary checks where I have arranged this privately to ensure they are registered/safe and reliable, and for any tuition remain in the room where possible, and ensure my child knows that tutors should not arrange new sessions or online chats directly with them**.
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
12. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed. I understand that s/he will be subject to sanctions if s/he does not follow these rules.

~~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____