Online Safety Policy

Written by	Sarah Hollywood & Angharad Prince
Date for review	February 2020
Signed by Headteacher	
Signed by SLT	
Review Dates confirmed	

Mission

"Come as you are, leave at your best"

Aim: The aim of this policy is to set out the ways in which the school will:
- educate all members of the school community about their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of Online Safety;
- work to empower the school community to use technology including the Internet as an essential tool for life-long learning.

Status: Statutory

Relationship to other policies: This Online Safety Policy is used in conjunction with other school policies, in particular the Child Protection & Safeguarding Policy and Acceptable Usage Agreements. We recognise the unique dignity of each person made in the image of God and our resulting responsibility to ensure the well-being of those in our care. Jesus had a particular care for children and the vulnerable and as a church school we see protecting members of our community from harm as a prime concern. We also recognise our responsibility not to allow the sharing of material which is exploitative or which demeans the dignity of any person. We see this as an issue of justice.

Table of Contents

Chapter 1 - Roles and Responsibilities

Role	Responsibilities
Governors	• Approve and review the effectiveness of the Online Safety Policy • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Online Safety Leader to share monitoring outcomes and report to the governors
Headteacher	• Ensure that all staff receive suitable CPD to carry out their Online Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring Online Safety incidents • Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or children • Inform the Local Authority about any serious Online Safety issues • Ensure that the school infrastructure / network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented
Online Safety and Computing Leader	• Monitor concerns logged by staff and inform others of Online Safety incidents, including the Online Safety Governor • Lead the establishment to review Online Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Acceptable Usage Agreements • Act in accordance with the Acceptable Usage Agreements and Online Safety Policy • Follow the school's reporting procedure to report any suspected misuse or problems to the Online Safety Leader • Follow Child Protection procedures for all serious concerns • Monitor technology use in lessons, extracurricular and extended school activities • Plan appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum • Respond to opportunities to model and discuss Online Safety
Children	• Read, understand and sign the agreed school Acceptable Usage Agreement (SMART rules) • Participate in Online Safety activities, follow the SMART rules and report any suspected misuse • Understand that following the SMART rules protects them out of school, including time spent on electronic devices • Support their friends to use the Internet responsibly and safely
Parents and Carers	• Endorse *(by signature)* the Child Acceptable Usage Policy *(SMART Rules)* • Discuss Online Safety issues with their child/ren and monitor their home use of technology devices *(including mobile phones and games devices)* and the Internet • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any Online Safety concerns that relate to the school
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible • Create password protected accounts for staff members to access confidential information relating to pupils • Maintain and inform the Senior Management Team of issues relating to filtering • Keep up to date with Online Safety technical information and update others as relevant

Visitors	• Use digital devices only in line with their business and in areas where you they have been approved to do so
	• Do not take/use images of pupils unless approved to do so
	• Do not leave equipment unattended
	• Do not use digital devices belonging to the school unless approved to do so

Chapter 2 – Policy Communication

2.1   How the policy will be introduced to pupils

This will be taught through the Computing programme of study and as part of every subject whenever pupils are using the Internet or accessing digital devices. Ongoing issues will also be covered in school newsletters, via Twitter and through assemblies and workshops.

- All users will be informed that network and Internet use will be monitored.
- An Online Safety programme of study *(included in the bespoke curriculum planning documents for all year groups)* will be established across the school to raise the awareness and importance of safe and responsible Internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online Safety rules will be posted throughout school.
- Safe and responsible use of the Internet and digital technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

2.2   How the policy will be discussed with staff

It is important that all staff feel confident to use new technologies in teaching and the Online Safety Policy will only be effective if all staff subscribe to its values and methods. ICT use is widespread and all staff including administration, midday supervisors, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school Online Safety Policy.

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement, and regularly review the Acceptable Usage Agreements.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user and that misuse may result in punitive action.
- Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The school will highlight useful online resources which staff should use with children in the classroom.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

2.3   How parents' support will be enlisted

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school will help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, <mark>school prospectus</mark> , through Twitter and on the school website and summarised through various awareness raising articles on a regular basis.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This will include offering parental workshops with resources, links and suggestions for safe home Internet use, or highlighting Online Safety at other attended events *(e.g. class assemblies and productions).* Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.

Chapter 3 - Teaching and learning of Online Safety

3.1   Why Internet use is important

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions as well as maintaining an online presence to the wider community.
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.2   How Internet use benefits education

Benefits of using the Internet in education include:
- Access to worldwide educational resources;
- Educational and cultural exchanges between pupils worldwide;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with North Tyneside Council and DfE.
- Access to learning wherever and whenever convenient.

3.3   How Internet use can enhance learning

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3.4   How pupils learn how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Chapter 4 - Managing Information and Data Systems

4.1   How information systems security will be maintained

- Users must take responsibility for their network use and act reasonably *(e.g. the downloading or uploading of large files during the working day will affect the service that others receive)*
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used without specific permission.
- Unapproved software will not be allowed on any device.
- Files held on the school's network will be regularly checked.
- The Network Manager will review system capacity regularly.
- The use of user logins and passwords to access various sites and resources will be enforced.

4.2   How email will be managed

- Pupils and staff must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- For reporting safeguarding, wellbeing and pastoral issues staff should use CPOMS or email the Headteacher / Learning Mentor.

4.3   How published content will be managed

- The contact details on the website should be the school address, email and telephone number.

- Pupils' personal information must not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Chapter 5 - Digital Video and Images

5.1   How the use of digital images and videos will be managed

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images and videos on the Internet.

- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published on the Internet. The main vehicles for this are the school website and school Twitter account, but can also include approved third parties *(visits, visitors, local press etc).*
- When taking digital images and posting on school website and Twitter, staff should view this as an opportunity to model good practice with regards to the appropriate use of social media.
- 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.
- Care should be taken when taking digital/video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without adult permission.
- Pupils' full names must not be used anywhere on the school website or Twitter account. First names can be used in text only posts, but no child should be made identifiable by associating names with videos or images.

Chapter 6 - Social Networking

The rapid emergence of new technologies has brought about the opportunity to communicate with others in a variety of new ways. Increasingly, technology has become a vital part of both our working and our social lives and, when used responsibly, it can be a positive tool to enhance teaching and learning. However, as with many new developments, the widespread use of social networking sites, has implications for both individuals and institutions, none more so than schools. It is therefore important that as an educational establishment, we balance our duty of care to our staff and pupils with our duty to provide the best learning opportunities, while at the same time ensuring that we preserve our good reputation and that we meet our legal responsibilities.

6.1   Purpose

The intention of this policy is to ensure that employees' use of social networking sites:
- does, when used explicitly for the purpose, enhance student learning
- serves to maintain the positive working relationships which exist in school
- does not reduce our ability to effectively safeguard pupils
- does not expose individuals or the school to potential legal action
- does not bring the name of the school into disrepute.

6.2   Definition of 'social networking sites'

For the purposes of this policy, the term *'social networking'* refers to any websites or apps which allow individuals to interact with others, by sharing information, opinions, knowledge, interests, pictures, video clips or photographs. This includes sites such as Facebook, Instagram, Snapchat and Twitter but also covers other web-based services including podcasts, blogs, wikis and video sharing sites such as YouTube. Please note that this is not an exhaustive list; due to the rapid emergence of new sites, this policy is NOT limited to the named sites.

6.3   Scope

This policy applies to all staff who work at our school. This includes teachers at all levels of responsibility, supply staff, support staff, including part time support staff, governors, volunteers, external service providers who work with our pupils and contractors.

6.4   Our Expectations

Employees are personally responsible for the information they choose to publish online. Our school encourages all its staff to take care in protecting their privacy and that of the school, our pupils and their families.

The school regards all e-communications as being within the public domain, given that no one has control of the content once it is sent. In the light of this, online activities should reflect the same levels of respect, consideration, honesty and professionalism that a colleague would use in person and this should be consistent with the standards and expectations outlined in 'DFE teaching standards'. Similarly, personal views expressed concerning non-school issues should not be in conflict with our school's ethos and expectations. Racist or homophobic comments, for example, would be considered unacceptable on the basis that at as school we do not tolerate discriminatory attitudes.

6.5 Social networking during the school day

Social networking for purely social purposes should not take place during the school day, except for during an employee's designated break or lunch time. Personal devices should not be connected to the school wireless network.

Where social networking sites are being used for educational purposes *(school Twitter account),* this may take place at other points in the school day but it is expected that individuals posting items or information will have gained permission to do so from the Headteacher. Those with permission to post to sites such as Twitter will have previously agreed to adhere to a set of school standards included within this policy document.

The time spent using social networking sites, even if the aim is to enhance teaching and learning, should not be to the extent that it interferes with an employee's primary job responsibilities. The impact of its use should be measurable and commensurate with the amount of time given to this activity.

6.6   Identifying oneself as an employee of our school

In identifying oneself as an employee of our school on a social networking site, an individual could be seen as a representative of the school. This means that everything posted on to that individual's page has the potential to reflect on the school and our image. Any employee naming the school also takes on the responsibility of representing the school in a professional manner and must therefore ensure that

their profile and related content is consistent with how they wish to present themselves to colleagues, parents and pupils as well as being consistent with the image and ethos of the school.

6.7   References to school based issues and stakeholders

Discussions of school-based matters should be undertaken with caution. If an employee does express a view on a school-based matter, it is important that the employee makes it very clear that the view does not represent that of the school itself.

Care must also be taken in making reference to other staff, pupils, parents, governors or any other member of our school community. Our relationship with our stakeholders is crucial and could be damaged through the making of ill-considered comments. Pupils in particular should not be referred to by name and any negative comments about members of our school community should not be made. Images of colleagues should not be placed onto any online site without first gaining permission from that colleague. Images of colleagues should be removed immediately upon their request. If a colleague has any doubt about the appropriateness of a comment or posting, they should err on the side of caution. It is important to remember that posts are archived online and cannot be permanently deleted.

6.8   Confidential information

As a school, we often legitimately need to discuss confidential information with colleagues. This type of information should not be discussed or referred to, even implicitly, on social networking sites. This includes discussions on private messaging sections of these sites, which are not guaranteed to be a secure form of communication.

6.9   Safeguarding and Child Protection

Friendships with pupils It is our policy that employees are not personal 'friends' with current pupils on social networking sites. This is a measure to protect both pupils and also colleagues from malicious allegations.
Friendships with ex pupils
Employees may choose to be 'friends' on a social networking site with ex-pupils but, again, must remember that the content of their posts will reflect on them and may reflect on the school and others in the school community. It is also worth remembering that many pupils will still have siblings in the school who may well have access to their social network pages, as may their parents.

Posting of videos or photographs of pupils
Videos, photographs or any other images of pupils should not be posted on any online forum without first having received signed authorisation from the parents/guardians. However, the use of images of pupils on the school website, school Twitter account or for whole school publicity purposes, does not fall within the Social Networking Policy. In all circumstances, images which identify pupils as being members of our school should only be used with extreme care.

6.10   Copyright and other legal issues

Employees must comply with the law with regard to copyrights and plagiarism. The work of others should not be posted on sites without permission unless it is in the form of brief quotations, which comply with 'fair use' exceptions.

Employees must also consider their legal position with regard to libel and defamation of character. Writing defamatory statements can result in legal action, brought by the victim. Furthermore, the school may take its own action if it feels an employee has brought the school's name into disrepute.

6.11 Conclusion

Our school is keen to embrace emerging technologies, such as social networking sites. Our aim is not to discourage this use but merely to ensure that all of our school community, both staff and pupils, remain safe while doing so. This policy, along with Professional Development sessions offered throughout the year, seeks to ensure that staff are well informed, enabling them to use social networking sites, confident in their ability to protect themselves and our pupils.

Chapter 7 - Technical Infrastructure

The School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements

- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
- The downloading of executable files by users
- The installation of programs on school devices unless permission is given by the Computing Subject Leader
- The installation of up to date virus software

Access to the school network and Internet will be controlled with regard to:
- Users having clearly defined access rights to school ICT systems through group policies
- Adult users being provided with a username and password
- Children being provided with a username
- Users being made aware that they are responsible for the security of their usernames and passwords and must not allow other users to access the systems using their log on details
- Users must immediately report any suspicion or evidence that there has been a breach of security
- An agreed process being in place for the provision of temporary access for supply and trainee teachers onto the school system.
- Children will use age-appropriate online tools and activities which will be adult directed

The Internet feed will be controlled with regard to access controls, which fall into several overlapping types (commonly described as filtering):
- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate access.

The ICT System of the school will be monitored with regard to:
- The school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems
- Online Safety incidents being documented and where appropriate reported immediately to the Online Safety Leader who will arrange for these to be dealt with immediately in accordance with the Acceptable Usage Policy

It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using Internet access and that Acceptable Usage Agreements are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online and should recognise acceptable and unacceptable behavior, and be aware of a range of ways to report concerns about content.
Any material that the school believes is illegal must be reported to appropriate agencies such as North Tyneside Council /CEOP.

Websites which schools believe should be blocked centrally should be reported to North Tyneside Council. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with North Tyneside Council to ensure that filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Leader who will then record the incident and escalate the concern as appropriate.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as North Tyneside Council, Police or CEOP.

Chapter 8 - Data Protection

We will ensure that under the Data Protection Act 1998 all school personnel are able to access their personal data that is held about them. We believe it is our duty to respond to any request of access within 40 days. We aim to protect the right of school personnel to privacy in line with the Data Protection Act 1998.

We believe that all personal data covered by the Data Protection Act 1998 includes the school admission register, attendance registers, curricular records, assessment data, class lists, reports to parents, disciplinary records, school personnel files, financial information, and strategic and

improvement plans. We aim to fulfill our obligations under the Data Protection Act 1998. We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

Aims
- To allow all school personnel their right to have access to their personal data.
- To protect all school personnel's right to privacy in line with the Data Protection Act 1998.
- To work with other schools to share good practice in order to improve this policy.

Responsibility for the Policy and Procedure

8.1   Role of the Governing Body:

The Governing Body has:
- the responsibility to comply with the legal requirements of the Data Protection Act 1998; delegated powers and responsibilities to the Headteacher as 'Data Controller' for the school;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring that the school complies with all equalities legislation;
- nominated a designated Equalities governor to ensure that appropriate action will be taken to deal with all prejudice related incidents or incidents which are a breach of this policy;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- responsibility for ensuring all policies are made available to parents;
- responsibility for the effective implementation, monitoring and evaluation of this policy

8.2   Role of the Headteacher and Senior Leadership Team:

The Headteacher and the Senior Leadership Team will:
- ensure the school complies with the Data Protection Act 1998 and the eight data protection principles;
- ensure security measures and confidential systems are in place to protect personal data and pupil records;
- ensure all personal data is accurate and that inaccurate data is corrected or erased;
- ensure procedures are in place to deal with requests for access to personal data;
- ensure school personnel are aware of their rights;
- ensure school personnel are aware of their responsibilities
- provide leadership and vision in respect of equality;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy;
- report to the Governing Body on the success and development of this policy as required

8.3   Role of School Personnel

School personnel will:
- comply with all aspects of this policy;
- follow the safe and confidential system procedures that are in place to protect personal data and pupil records;
- receive a copy of their personal data at the beginning of every academic year:
- check this data and will inform the Data Controller of any mistakes;

- comply and respect confidentiality of personal information when involved with interviewing new school personnel;
- inform the school and the Local Authority of any changes to their personal data
- implement the school's equalities policy and schemes;
- report and deal with all incidents of discrimination;
- attend appropriate training sessions on equality;
- report any concerns they have on any aspect of the school community

8.4 Raising Awareness of this Policy

We will raise awareness of this policy via media such as:
- the School Handbook/Prospectus
- the school website and Twitter account
- the Staff Handbook
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- school events
- meetings with school personnel
- communications with home such as weekly newsletters and half-termly newsletters
- reports such annual report to parents and Headteacher reports to the Governing Body
- information displays around school

8.6 Data Protection Principles

Personal data must:
- be processed lawfully;
- be obtained and processed for specific and lawful purposes;
- be sufficient, appropriate and not excessive in relation to the precise purpose;
- be accurate and up to date;
- not be kept for a great length of time;
- be processed in agreement with the individual's legal rights;
- be protected against unlawful processing, accidental loss, destruction or damage;
- not be transferred outside the EU unless the rights and freedom of the individual is protected

8.6 Security Measures

We work in conjunction with the Local Authority Code of Practice to ensure that computers and servers comply with all up to date Government regulations and are secure with:
- anti-virus software;
- fire wall software;
- passwords

All school personnel are trained to:
- be discreet and confidential;
- consider the safe and secure positioning of digital devices;
- back up data;
- turn off computers when not in use;
- remember password access;
- lock filing cabinets and doors to offices;
- shred confidential material;

8.7 Disclosure of Data

Personal data cannot be disclosed to a third party without the consent of the individual except when it is legally required.

8.8 Requests for Access to Data

All requests from school personnel for access to their data must be made in writing on headed note paper and sent to the data controller.

8.9 Rights of Individuals

Individuals have rights to:
• know when their data is being processed, the reason it is being processed and the name of the person or organisation requesting the information;
• prevent processing which could be harmful to them or others;
• prevent the processing of their performance management records;
• go to court to prevent inaccurate data being used;
• be compensated if a data controller contravenes the Data Protection Act;
• stop data being processed for direct marketing

Individuals are not entitled
to: ▄ copies of their
references;
• information on pay reviews;
• examination results until they have been released

8.10 Grievance Procedure

Any member of the school personnel who disputes any aspect of their personal data with the Data Controller has the right to take up the matter under the school's formal grievance procedures.

8.11 Training

We ensure all school personnel have equal chances of training, career development and promotion. Periodic training will be organised for all school personnel so that they are kept up to date with new information and guide lines concerning equal opportunities.

8.12 Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

8.13 Monitoring the Effectiveness of the Policy

The practical application of this policy will be reviewed when the need arises by the coordinator, the Headteacher and the nominated governor. A statement of the policy's effectiveness and the

Chapter 9 - Bullying (including Online Bullying)

9.1   Introduction

It is a Government requirement that all schools have an anti-bullying policy. The school policy reflects this and DfE advice.

DfE guidance defines bullying as actions that are meant to be hurtful, and which happen on a regular basis. Bullying can be direct (either physical or verbal) or indirect (for example, being ignored or not spoken to).

9.2   Aims and objectives

Bullying is wrong and damages individual children. We therefore do all we can to prevent it, by developing a school ethos in which bullying is regarded as completely unacceptable.

We aim, as a school, to produce a safe and secure environment where all can learn without anxiety, and measures are in place to reduce the likelihood of bullying.

This policy aims to produce a consistent school response to any bullying incidents that may occur.

We aim to make all those connected with the school aware of our opposition to bullying, and we make clear each person's responsibilities with regard to the eradication of bullying in our school.

9.3   The role of governors

The governing body supports the Headteacher in all attempts to eliminate bullying from our school. The governing body will not condone any bullying at all in our school, and any incidents of bullying that do occur will be taken very seriously, and dealt with appropriately.

The governing body monitors incidents of bullying that do occur, and reviews the effectiveness of this policy regularly. The governors require the Headteacher to keep accurate records of all incidents of bullying, and to report to the governors on a yearly basis about the effectiveness of school anti-bullying strategies.

A parent who is dissatisfied with the way the school has dealt with a bullying incident can ask the chair of governors to look into the matter. The governing body responds within ten days to any request from a parent to investigate incidents of bullying. In all cases the governing body notifies the Headteacher, and asks her to conduct an investigation into the case, and to report back to a representative of the governing body. The governing body then report their findings to the parent.

9.4   The role of the Headteacher

It is the responsibility of the Headteacher to implement the school anti-bullying strategy, and to ensure that all staff (both teaching and non-teaching) are aware of the school policy, and know how to identify and deal with incidents of bullying. The Headteacher reports to the governing body about the effectiveness of the anti-bullying policy on request. The anti-bullying policy will usually form part of the induction process for new staff.

The Headteacher ensures that all children know that bullying is wrong, and that it is unacceptable behaviour in this school. The Headteacher draws the attention of children to this fact at suitable moments. For example, if an incident occurs, the Headteacher may decide to use an assembly as the forum in which to discuss with other children why this behaviour was wrong, and why a pupil is being punished.

The Headteacher ensures that all staff, including lunchtime staff, receive sufficient training to be equipped to identify and deal with all incidents of bullying.

The Headteacher sets the school climate of mutual support and praise for success, so making bullying less likely. When children feel they are important and belong to a friendly and welcoming school, bullying is far less likely to be part of their behaviour.

9.5 The role of the teacher and support staff

All the staff in our school take all forms of bullying seriously, and seek to prevent it from taking place.

Teachers keep their own records of all incidents that happen in their class, and that they are aware of in the school. If teachers witness an act of bullying, they will either investigate it themselves and always refer it to the Headteacher. Teachers and support staff do all they can to support the child who is being bullied. If a child is being bullied over a period of time, then, after consultation with the Headteacher, the teacher informs the child's parents.

When any bullying takes place between members of a class, the teacher will deal with the issue immediately. This may involve counselling and support for the victim of the bullying, and punishment for the child who has carried out the bullying. Time is spent talking to the child who has bullied: explaining why his/her action was wrong, and that child is encouraged to change his/her behaviour in future. If a child is repeatedly involved in bullying other children, we inform the Headteacher and the special needs coordinator. We then invite the child's parents into the school to discuss the situation. In more extreme cases, for example where these initial discussions have proven ineffective, the Headteacher may contact external support agencies, such as the social services.

All members of staff routinely attend training, which equips them to identify bullying and to follow school policy and procedures with regard to behaviour management.

Teachers use a range of methods to help prevent bullying and to establish a climate of trust and respect for all. They use drama, assemblies, role-play, stories etc, within the formal curriculum, to help pupils understand the feelings of bullied children, and to practise the restraint required to avoid lapsing into bullying behaviour. Time in class is used to praise, reward and celebrate the success of all children, and thus to help create a positive atmosphere.

9.6 The role of parents

Parents who are concerned that their child might be being bullied or who suspect that their child may be the perpetrator of bullying, should contact their child's class teacher immediately. If they are not

satisfied with the response, they should contact the Headteacher. If they remain dissatisfied, they should follow the school's complaints procedure, as detailed in the school Prospectus.

Parents have a responsibility to support the school's anti-bullying policy, actively encouraging their child to be a positive member of the school.

9.7 The role of pupils

Pupils are encouraged to tell anybody they trust if they are being bullied, and if the bullying continues, they must keep on letting people know.

Pupils are invited to tell us their views about a range of school issues, including bullying, in the annual pupil questionnaire.

9.8 Online Bullying

Online Bullying can be defined as ***"The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone"*** DCSF 2007

The DFE 2017 note that "The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click". Preventing and Tackling Bullying.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles devices, social media, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand Online Bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how Online Bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Online Bullying *(along with all other forms of bullying)* of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
• There are clear procedures in place to support anyone in the school community affected by Online Bullying.
• All incidents of Online Bullying reported to the school will be recorded.
• There will be clear procedures in place to investigate incidents or allegations of Online Bullying under the Bullying Policy
• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
• The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
• Pupils, staff and parents/carers will be required to work with the school to support the approach to Online Bullying and the school's Online Safety ethos.

Sanctions for those involved in Online Bullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offense is suspected.

9.9 Monitoring and review

This policy is monitored on a day-to-day basis by the Headteacher, who reports to governors on request about the effectiveness of the policy.

Chapter 10 - Mobile Devices

Staff are allowed to bring mobile phones into school but they must only use them during break, lunchtimes or during non-contact when they are not in contact with children unless they have the permission of the Headteacher. These must be turned off or onto silent during the school day. They are not allowed to use personal devices to take photographs or videos in school for any purpose without the express permission of the Senior Management Team.

Staff should not use their personal mobile devices to contact children, parents and carers. Use for school trips is an exception but the Headteacher will be informed of their use.

Children who bring mobile phones into school should hand them into their class teacher at the start of the day and they will then collect them again at the end of the school day.

Chapter 11 - Policy Decisions

11.1 How Internet access will be authorised

- All staff will read and sign School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- Pupils will use age-appropriate online activities will be teacher-directed where necessary.

11.2 How risks will be assessed

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device. Neither the

school norNorth Tyneside Council can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

11.3   How the school will respond to any incidents of concern

Online Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Pupils are the first line of defence; being encouraged to report issues and concerns and immediately, and then schools staff using their observation of behaviour which is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff and pupils should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. Assuming that the Headteacher is not the subject of concern, a decision to escalate would normally sit with the Headteacher and the decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or Online Safety officer, if the offence is deemed to be out of the remit of the school to deal with. Staff should however be encouraged to take matters further if they are NOT satisfied with leaders responses.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns *(such as breaches of filtering, Online Bullying, illegal content etc).*
- The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or Online Safety Officer and escalate the concern to the Police

11.4   How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.

11.5 How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the Internet and technology whilst on the school site.
- In accordance with the Computing programme of study, the school will educate children on how to use technology safely and respectfully, impacting on school, home and community behaviour.

11.6 How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of theNetwork by pupils and staff in all areas, in particular message and communication tools and publishing facilities such as blogging.
- Pupils/staff will be advised about acceptable conduct and use when using the Network
- Only members of the current pupil, parent/carers and staff community will have access to the Network.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Network.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

New York Primary School
Come as you are. Leave at your best.

Online Safety

Follow the SMART rules to stay safe online

S Stay safe online by not sharing personal information

M Do not meet anyone who you have only made friends with online

A Do not accept messages or friend requests from strangers

R Not everything online is reliable. Some people online are strangers and may try and trick us

T Tell an adult you trust if anything happens online that you dont like

Chapter 12 – Acceptable Usage Agreements

The Acceptable Usage Agreements reflect the school Online Safety Policy.

The school will ensure that staff and visitors will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and visitors to agree to be responsible users.

The Acceptable Usage Agreements apply to staff and visitors who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

The following Acceptable Use Agreements are in place and are attached for reference to this policy:

- Staff Acceptable Use Agreement

- Staff iPad Acceptable Use Agreement

- Staff Laptop Acceptable Use Agreement

- Visitor Agreement (including acceptable usage of digital devices)

- Parent and Carer Acceptable Use Policy

- Children's Acceptbale Use Policy (SMART Rules)

New York Primary School
Staff Acceptable Use Agreement

This Acceptable Use Agreement reflects the school Online Safety Policy.

The school will ensure that staff and visitors will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and visitors to agree to be responsible users.

This Acceptable Use Agreement applies to staff and visitors who have access to and are users of school ICT systems and to school related use of ICT systems outside of school.

Responsibilities
I agree to:
- read, understand, sign and act in accordance with the School Online Safety policy.
- report any suspected misuse or problems to the Headteacher.
- monitor ICT activity in lessons, extracurricular and extended school activities.
- model the safe use ICT.
- refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the school or may bring the school into disrepute *(including personal sites).*

Education
- I understand that I am responsible for the Online Safety education of children.
- I will respect copyright and educate the children to respect it as well.

Training
- I understand that I will participate in Online Safety training.
- I understand that it is my responsibility to request training if I identify gaps in my abilities.

Online Bullying
- I understand that the school has a zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures.

Technical Infrastructure
I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:
- the proxy or firewall settings of the school network *(unless I have permission).*
- not having the rights to install software on a digital device *(unless I have permission).*

Passwords
- I will only use the password(s) given to me.
- I will never log another user onto the system using my login.

Filtering
- I will not try to by-pass the filtering system used by the school.
- If I am granted special access to sites that are normally filtered, I will not leave my digital device unsupervised.
- I will report any filtering issues immediately.
- I understand that the school will monitor my use of digital devices and the Internet.

Data Protection
- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up.

Use of digital images
I will follow the school's policy on using digital images making sure that:
- only those children whose parental permission has been given are published.
- full names of pupils are not used and that no child is ever identifiable from a photograph.

Communication
- I will be professional in all my communications and actions when using school ICT systems.

Email
- I will use the school provided email for all business matters.
- I will not open any attachments to emails, unless the source is known and trusted *(due to the risk of the attachment containing viruses or other harmful programmes).*

Personal publishing
- I will follow the Online Safety policy concerning the personal use of social media.

Mobile Phones
- I will not use my personal mobile phone during contact time with children.
- I will not use my personal mobile phone to contact children or parents with the exception of school trips where the Headteacher must be informed of their use.

Reporting incidents
- I will report any suspected misuse or problems to the Online Safety Leader.
- I will follow Child Protection procedures for all serious concerns.
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary procedures
- I understand that there are regulations in place when children use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the School ICT systems in any way then there are disciplinary procedures that will be followed by the school.

Staff Acceptable Use Policy

I have read, understood and agree to abide by the terms of the Staff Acceptable Use Policy.

Name:………………………………………………………………………………….…..

Signature:……………………………………………………… Date:.…………………………

Headteacher signature:………………………………… Date:………………………….

New York Primary School
iPad Acceptable Use Agreement

The iPads are to be used for professional purposes only and staff must bring their iPad to school every day, fully charged.

All users of the iPads will be required to review this AUP and sign the bottom of the form in order to demonstrate an understanding of these rules. iPad users will also agree to follow all relevant policies and procedures, be role models, display good practice and provide leadership in the use of these devices.

Staff use of the iPad falls under the guidelines of our Acceptable Use Policy for technology. Access to the Internet is monitored through our school's content filtering software and all rules and expectations are applied to the use of the iPad. All applications, images, videos and documents stored on the iPad are the property of School and are subject to regular review and monitoring.

Staff will be provided with an iPad, USB Cable, USB Charger and case. The iPad must be surrendered to New York Primary School in appropriate working condition, immediately upon termination of employment or at the request of the Headteacher. New York Primary School reserves the right to require the return of an iPad from a staff member at any time and without notice.

At all times the iPad shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and email.

Individual users are responsible for the setting up of any home Internet connection to use in conjunction with the iPad and no support will be provided for this by the school.

The following guidelines are general in nature as not every possible scenario can be thoroughly described or known at this point in time.

Maintenance and Care of Devices

- Staff issued with an iPad are expected to exercise the same care in respect of the security and upkeep of the iPad as if it were the employee's own property.

- Malfunctions or any other technical problems *(either hardware or software related)* should be reported immediately to the Headteacher, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible. Under no circumstances is the employee to organise repairs to the iPad before reporting the problem.

- You (and only you) may take the iPad off-site if you plan to use it in a way that will benefit the school. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments. If the iPad is lost or damaged as a result of neglect on behalf of the staff member, then you may be responsible for a contribution towards the replacement of the device.

- The iPad screens are particularly sensitive to damage from excessive pressure on the screen. Users must avoid placing too much pressure and/or weight *(such as folders and workbooks)* on the screen in order to refrain from any unnecessary damage.

- The iPad must not be subjected to extreme heat or cold.

- Users must take responsibility for installing software updates *(updates provide important security settings and it is therefore essential that these are installed).*

- Users must keep the iPad clean and in good working order.

Security and Privacy

- It is a user's responsibility to keep their iPad safe and secure. When iPads are left unattended they must be stored in a safe place around school.

- It is a user's responsibility to ensure that their allocated iPad is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the iPad in a communal area, any off-site venue and whilst travelling.

- iPads must not be left unattended or on view in motor vehicles at any time.

- If the iPad is lost, stolen or damaged, the Headteacher must be notified immediately. If necessary, the device will be remotely locked and/or wiped. New York Primary School is not responsible for the loss of any personal files that may be deleted remotely from an iPad.

- The use of 'Jailbreaking' is strictly prohibited *('Jailbreaking' is the process which removes any limitations placed on the iPad by Apple, resulting in a less secure device).*

- Users are required to set up a passcode lock to keep the device protected. This code is strictly confidential and must not be divulged to other staff or pupils.

- You must ensure that your school email account has been enabled on your iPad and that you have checked your email prior to the commencement of the school day. This is now our main source of group communication and is therefore essential that you check your email account on a regular basis.

- Along with the Acceptable Use Policy, staff must adhere at all times to the Data Protection Act (1998), The Computer Misuse Act (1990) and the school's health and safety policy when using iPads in school.

- When using iPads with pupils it is your responsibility to ensure that children are not accessing confidential information.

- Users may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations.

- Staff may not use the Internet to view illegal or inappropriate material that would place the member of staff or school at legal risk.

- Staff are responsible for looking after their iPad. When left unattended they must be stored out-ofsight. The whereabouts of this iPad should be reported to the Headteacher, but not be divulged to adults or pupils outside your class team.

Applications

- You have the ability to download FREE apps which you feel may be of benefit to you, or the pupils in your class. An *'App Request Form'* should be completed for any **'paid'** apps which you require to be installed.

- Staff should be aware that the school, via its management system, can see what apps have been installed on the iPads.

- Updates to applications can be carried out by teaching staff, when required.

- Memory space is limited and academic content takes precedence over personal files and apps.

Social Media

- For the purposes of this policy, social media includes *(but is not limited to)* Internet forums, blogs, wikis, podcasts, photograph websites *(Flickr, Instagram, Snapchat, etc.)*, Facebook and Twitter. Staff should follow these guidelines in relation to any social media applications that they use, both in work and in their personal lives.

- Users should not access social media applications from the school's iPads when working in school unless it is for educational purposes *(school Twitter account).*

- Users should understand that anything they write *(regardless of privacy settings)* could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.

Use of Digital and Video Images

- Staff using iPads must be aware of the risks associated with sharing images and videos on the Internet.

- Users must make good judgment when using the iPad camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.

- Staff must not take, use, share, publish or distribute images of others without their permission.

- Inappropriate media may not be used as a screensaver or background photo.

- Deletion of photos and videos may be instructed periodically by the Headteacher or if a device's memory is full.

iPad Acceptable Use Policy

I have read, understood and agree to abide by the terms of the iPad Acceptable Use Policy.

 iPad Serial Number:............…………………………………………………………..

Name:…………………………………………………………………………..…..

Signature:……………………………………………………   Date:.…………………………

Headteacher signature:…………………………………   Date:………………………….

New York Primary School
Visitor Agreement

We are committed to safety and wellbeing of all pupils/students, staff and visitors therefore all visitors must agree to the following before being allowed access to the whole School site.

GENERAL	• Enter and exit the site from the main entrance, observe signing in and out procedures. • Do not move around the school site unescorted. Please stay within the areas that are necessary for your visit. • You will be issued with a 'Visitors' badge, this must be worn at all times so that it is visible. Please return this to Reception as you leave the School site. • Accessible adult toilets are located in the corridor between the staffroom and the main hall. • First aid equipment is stored in the designated areas for use by visitors.
FIRE	• The fire alarm is tested every Thursday at 4pm, if you hear the alarm at any other time please leave by the nearest exit. • Report to the nearest fire assembly point so that you can be accounted for. • If you are working with pupils, please familiarise yourself with the fire evacuation procedures (displayed on classroom walls) and in the event of the alarm sounding, lead them to safety and inform a member of school staff so that registers may be taken.
DIGITAL DEVICES	Whilst on site please: • Use only in connection with your business and when and where you are approved to do so (e.g. staffroom). • Do not take/use images of children unless approved to do so. • Do not leave equipment unattended. • Do not use mobile phones in the presence of pupils. • Digital devices belonging to the school are not to be used by visitors, unless you are approved to do so.
INTERACTION WITH PUPILS	Where your role requires that you interact with pupil or you are attending School on Local Authority/Agency working you must: • Present your photo ID (and any documentation previously agreed between school and the Local Authority/Agency) when requested by our Reception Staff. • Wear your Photo ID and Visitor's Badge at all times when on the School site. • Interact with pupils as required within your professional capacity and report and instances/concerns/observations you may have immediately to a senior member of school staff (Office staff will provide advice on how to make this contact if appropriate).

Anyone whose actions/behaviours, etc causes concern or who do not follow the above requirements will be reported to the Local Authority for further action.

Please sign below when you have read all the above criteria.

Signed: _____   **Print Name: _____**

Date: _____   **Time: _____**

New York Primary School
Parent and Carer Acceptable Use Agreement

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.

The Internet will be used within school to support children's learning both *formally (within taught lessons)* and informally *(outside taught lessons),* at the discretion of a member of staff who will set guidelines and rules for its use. Children will be taught to be critical in their use of Internet sites.

Children may have opportunities to communicate with others through Twitter and via messages and blogs on the eSchools platform. This will only take place in accordance with the school's policy and procedure, so their full name will never appear online. Responsible and considerate language will be used at all times in communicating with others.

Children will:
- only use the school digital devices for those activities which they have been given permission to use and under the appropriate supervision of a member of staff.
- be made aware of what online bullying is and what to do if it happens.
- only use the user names and passwords they have been given
- not download and use material which is copyrighted or plagiarise content from the Internet.
- not attempt to search for, view, upload or download any material that is likely to be unsuitable in a school or is blocked by the school's filter.
- inform a member of staff if they have accidentally accessed inappropriate content.
- use responsible and considerate language in communicating with others.
- be encouraged to discuss their use of digital devices, their amount of screen time and their use of sites and apps that are age specific *(especially in relation to Social Network sites).*
- hand in mobile phones to the office upon entering school and collect them again at the end of the school day.
- be encouraged to talk with their parents or carers about the rules for Online Safety.
- be made aware that the school may investigate incidents that happen outside of school but could have an effect on the school.

Failure to comply with these rules will result in one or more of the following:
- A ban, temporary or permanent, on the use of the Internet at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on future access to school facilities.

If you do not understand any part of this document, you should ask a member of staff for guidance.

If you have any concerns regarding this policy, the form below must be completed, signed and returned to the school for our records.

Parent's name:	
Child's name:	
Class:	
Date:	
Comments:	

New York Primary School
Children's Acceptable Use Agreement

Technology is a fantastic resource to support learning within school and to communicate with others. The School encourages its appropriate, effective and safe use. All users of technology and devices in school must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities
- I understand that I have rights and responsibilities in using ICT and will act responsibly when using technology, digital devices or the Internet.
- I will learn the school's SMART rules to keep myself safe inside and outside of school • I will report any suspected misuse or problems to a teacher or trusted adult within school.
- I will make sure there is permission to use any material that I find *(i.e. copyright).*

Communication – (eSchools, email, Twitter, blogging, Skype etc.)
- I will be careful in my communications making sure that nothing I write is offensive, and that it is considerate.
- I will not write anything that could be seen as insulting to the school.

Online Bullying
- I understand that the school will not accept bullying in any form.
- I will be careful with all communications making sure that anything I write is considerate and could not be interpreted as bullying.
- I understand that I should report any incidents of bullying and know how to do this.

Our School SMART Rules

Child's name:	
Signature:	
Class:	
Date:	