Policy Approved at Governors: December 2017	Due for renewal: December 2018

NORTH NEWTON COMMUNITY PRIMARY SCHOOL

ONLINE SAFETY POLICY INCLUDING COMPUTING, FREEDOM OF INFORMATION, DATA PROTECTION, PRIVACY NOTICE AND STAFF AND VOLUNTEER ACCEPTABLE USE POLICY

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of online;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

The Online Safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place.

Scope of policy
This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as online-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school.

The school will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review
The impact of the policy will be monitored by the governors by looking at:

- the log of reported incidents
- the Internet monitoring log
- surveys of staff, parents and children
- other documents and resources
- future developments

Roles and responsibilities
The Headteacher, Senior Teacher and Governors oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The Online Safety Leader will work with the Headteacher/ Designated Safeguarding Lead to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation), inappropriate online contact with adults, potential or actual incidents of grooming and online-bullying.

An online working group will work with the Online Safety Leader to implement and monitor the online policy and AUPs (Acceptable User Policies). This group is made up of Online Safety Leader, Safeguarding Lead, teacher, governor, member of support staff, member of senior leadership team and pupils. Pupils are part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	• Approve and review the effectiveness of the online Policy • Delegate a governor to act as online link • Online Governor works with the online Leader to carry out regular monitoring and report to Governors • Ensure systems are in place that to identify children accessing or trying to access harmful and inappropriate content online
Head Teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their online roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive online curriculum in place • Ensure that there is a system in place for monitoring online safety • Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil • Inform the local authority about any serious online 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 • Use an audit to annually review online with the school's technical support
Online Leader	• Lead the online working group • Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of online policies and documents • Lead and monitor a progressive online safety curriculum for pupils • Ensure all staff are aware of the procedures outlined in policies relating to online safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA online safety staff and technical staff

	• Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Safeguarding lead
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and online Safety Policy • Report any suspected misuse or concerns to the Online Safety Leader and check this has been recorded • Provide appropriate online safety learning opportunities as part of a progressive online safety curriculum and respond • Model the safe and effective use of technology • Monitor ICT activity in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand and sign the Pupil AUP and the agreed class Internet rules • Participate in online safety activities, follow the AUP and report concerns for themselves or others • Understand that the Online Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss online safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any online issues that relate to the school • Maintain responsible standards when using social media to discuss school issues
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with online technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can

	be reported to the Online Safety Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities

Education of pupils
Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to Online Safety'

School Inspection Handbook - Ofsted 2014
A progressive planned online safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Breadth and progression is ensured through implementation of the Somerset ActiveBYTES scheme and the Online Safety progression that is part of the Somerset Primary Computing Curriculum/Somerset Byte Guide to SWGfL Digital Literacy Materials for KS3 and 4.

Within this:

- key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset ActiveBYTES scheme of work
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- pupils are taught to be critically aware of the content they access online, including recognition of extreme and commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology
- pupils will write and sign an AUP for their class [which might be agreed class rules] at the beginning of each school year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including online-bullying'

Education and information for parents and carers
Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates;

- raising awareness through activities planned by pupils;
- inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate;
- providing and maintaining links to up to date information on the school website

Education of wider school community
The school provides information about Online Safety to organisations using school facilities, local play groups and nurseries and members of the wider community which where appropriate include:

- details about the Online Compass review tool
- Online Safety messages targeted to grandparents and other relatives

Training of Staff and Governors
There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- an annual audit of the Online Safety training needs of all staff
- all new staff and governors receiving Online Safety training as part of their induction programme
- providing information to supply and student teachers on the school's Online Safety procedures
- the Online Safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the Online Safety Leader providing guidance and training as required to individuals and seeking LA support on issues
- staff and governors are made aware of the UK Safer Internet Centre helpline 0344 381 4772

Online bullying
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.

The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111.

Pupils, staff and parents and carers will be encouraged to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of online bullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and 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 will follow those for other bullying incidents and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

- internet access being suspended at the school 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 AUP

- the parent and carers of pupils being informed

- the police being contacted if a criminal offence is suspected

Sexting
The school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an intimate sexting image or is suspected of having such an image, will be secured and switched off. This will then be reported to the safeguarding lead. An individual member of staff will not investigate, delete or pass on the image. The safeguarding lead will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking can be put into place.

Technical Infrastructure
The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- 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 and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

o the downloading of executable files by users

o the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school

o the installing of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator

o the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)

o the installation of up to date anti-virus software

- access to the school network and internet will be controlled with regard to:

o users having clearly defined access rights to school ICT systems through group policies

o users (apart from possibly Foundation Stage and Key Stage One pupils) being provided with a username and password

o staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details

- o the 'master/administrator' passwords are available to the Headteacher and kept in the school safe

- o users must immediately report any suspicion or evidence that there has been a breach of security

- o an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this Online Safety policy

- o Key Stage 1 pupils' access will be supervised with access to specific and approved online materials

- o Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities

- the internet feed will be controlled with regard to:

- o the school maintaining a managed filtering service provided by an educational provider that includes filtering of terms related to terrorism

- o the school monitoring internet use, being aware of the websites that are used and attempts to access inappropriate or illegal sites

- o requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using a proforma

- o requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged

- o filtering issues being reported immediately

- the IT System of the school will be monitored with regard to:

- o the school IT technical support regularly monitoring and recording the activity of users on the school IT systems

- o Online Safety incidents being documented and reported immediately to the Online Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP.

DATA PROTECTION

The schools Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

- at all times take care to ensure the safe keeping of personal data and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups.

- use personal data only on secure password protected computers and other devices

- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data

- store or transfer data using approved services such as remote access, the Somerset Learning Platform (SLP), encryption and secure password protected devices

- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection officer

- check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images both on school devices and personal devices where permission has been given by the Headteacher
- make sure that images or videos that include pupils will be selected carefully with their knowledge
- seek permission from parents or carers before images or videos of pupils are electronically published
- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission
- Help all parties to recognise that any published image could be reused and repurposed
- make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use
- publish a policy regarding the use of photographic images of children which outlines policies and procedures including disposal and deletion

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- use email at KS1 through a group or class activity with an adult sending and opening emails
- provide pupils at Key Stage 2 with a monitored individual educational school email addresses

- teach pupils about email safety issues through the scheme of work and implementation of the AUP

- only publish official staff email addresses where this required

with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school

- control access to social media and social networking sites in school

- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences

- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given

- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team

- ensure that any digital communication between staff and pupils or parents and carers is always professional in tone and content

- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards 2012

- staff are advised that no reference should be made to pupils, parents/carers or school staff

- advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory

- register concerns (e.g. recording in online log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites

- support staff to deal with the consequences of hurtful or defamatory posts about them online

- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team

with respect to mobile phones

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Headteacher

- inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team

- inform all that personal devices should be password protected

- advise staff not to use their personal mobile phone to contact pupils, parents and carers

- provide a mobile phone for activities that require them

- inform visitors of the schools expectations regarding the use of mobile phones
- allow pupils to bring mobile phones into school but only for use at specified times and for approved activities
- maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

with respect to other personal devices

- encourage pupils to bring their own device to support planned learning experiences
- ensure pupils using their own device sign an addition to the pupil AUP to agree to responsible use
- ensure that staff understand that the AUP will apply to staff using their own portable device for school purposes
- enable and insist on the use of the school's Internet connection while on the school site
- maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

Prevent Duty

Statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in school. As a school, we have suitable filtering in place and children are told what to do if they access something online which they know is not appropriate.

As a school we have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety is integral to North Newton's computing curriculum and will also be embedded in PSHE.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults			Pupils		
Communication Technologies	Allowed	Allowed for selecte staff	Not allowed	Allowed	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x					x
Use of mobile phones in lessons			x			x
Use of mobile phones in social time	x					x
Taking photos on mobile phones or other camera devices (ie iPads)			x			x
Use of personal devices	x				x	

Use of personal email addresses in school, or on school network	x				x	
Use of school email for personal emails			x			x
Use of chat rooms / facilities			x			x
Use of messaging apps	x				x	
Use of social networking sites	x					x
Use of blogs	x				x	
Use of Twitter	x				x	
Use of video broadcasting eg Youtube		x			x	

Assessment of risk
Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the online safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate 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 computer. Neither the school nor Somerset County Council can accept liability for the material accessed, or any consequences resulting from Internet use.

All users need to be reminded that 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.

Reporting and Response to incidents
The school will follow Somerset's flowcharts to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of Child abuse then the monitoring will be halted and referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- The Online Safety Leader will record all reported incidents and actions taken in the School Online Safety incident log and in any other relevant areas e.g. Bullying or Safeguarding log
- The designated Safeguarding Lead will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage online safety incidents in accordance with the School Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- 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 Somerset Children Safeguarding Team and escalate the concern to the police

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser or Local Authority Designated Officer (LADO)

If an incident or concern needs to be passed beyond the school then the concern will be escalated to the Safeguarding for Schools Adviser to communicate to other schools in Somerset. Should serious online safety incidents take place, the following external persons and agencies should be informed:	Safeguarding for Schools Adviser Jane Weatherill *Via Somerset Direct where pupil involved* Local Authority Designated Officer (LADO) Anthony Goble *Via Somerset Direct where staff involved* Police

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false.

Sanctions and Disciplinary proceedings
Sanctions and disciplinary procedures may be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation (p 17):

- Child Sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files

- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet

In addition the following indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)			x	
Online gaming (non-educational)				x
Online gambling				x
Online shopping / commerce			x	
File sharing (using p2p networks)			x	

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore ticks may appear in more than one column. The ticks in place are actions which must be followed.

Incidents	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Inform parents / carers	Removal of network / Internet acce rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	x	✓	✓	X	X	
Unauthorised use of non-educational sites during lessons	X	X		X	X	X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X		X	X	X	
Unauthorised use of social networking / instant messaging / personal email	X	X		X	X	X	
Unauthorised downloading or uploading of files	X	X		X	X	X	
Allowing others to access school network by sharing username and passwords	X	X		X	X	X	
Attempting to access or accessing the school network, using another pupil's account	X	X		X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X		X	X	X	
Corrupting or destroying the data of other users	X	X		X	X	X	
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature	X	X		X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X		X	X	X	X

Using proxy sites or other means to subvert the school's filtering system	x	x		x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x		x	x	x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x		x	x	x	

Sanctions: Staff

Incidents:	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff fc action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	x	x	L,P		x		x
Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email	x	x			x		x
Unauthorised downloading or uploading of files	x	x		x	x		x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x			x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x			x		x
Deliberate actions to breach data protection or network security rules	x	x			x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff	x	x			x		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	x	x	L		x		x
Breech of the school online policies in relation to communication with learners	x	x	L		x		x
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils?	x	x	L	x	x		x
Actions which could compromise the staff member's professional standing	x	x			x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x			x		x
Using proxy sites or other means to subvert the school's filtering system	x	x		x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	L	x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	L	x	x	x	x
Breaching copyright or licensing regulations	x	x		x	x		x
Continued infringements of the above, following previous warnings or sanctions	x	x		x	x		x

FREEDOM OF INFORMATION

Introduction
North Newton School is committed to the Freedom of Information Act (FoI) and to the principles of accountability and the general right of access to information. This policy outlines our response to the Act and a framework for managing requests.

Background
The school recognises that under the FoI, any person (the enquirer) has a legal right to ask for access to information held by the school. The enquirer is entitled to be told whether the school holds the information, and to receive a copy, subject to certain exemptions.

The information which the school routinely makes available to the public is included in the Publication Scheme. Requests for other information will be dealt with in accordance with the statutory guidance.

As requests under FoI can be addressed to anyone in the school all staff will be made aware of the process for dealing with requests.

The school will respond to all requests, telling the enquirer whether or not the information is held, and supplying any information that is held, except where exemptions apply.

The school will respond to each request within 20 days excluding school holidays.

Scope
If any element of a request to the school includes personal or environmental information, these will be dealt with under the Data Protection Act (DPA) or Environmental Regulations (EIR). Any other information is a request under FoI, and must be dealt with accordingly.

Requests for information about anything relating to the environment – such as air, water, land, the natural world or the built environment and any factor or measure affecting these – are covered by the EIR. They also cover issues relating to Health and Safety. Requests under EIR are dealt with in the same way as those under FoI, but unlike FoI requests, they do not need to be written and can be verbal.

Obligations and Duties
The school recognises its duty to

- provide advice and assistance to anyone requesting information. The school will respond to straightforward verbal requests for information, and will help enquirers to put more complex verbal requests into writing so that they can be handled under the Act.
- tell enquirers whether or not we hold the information they are requesting (the duty to confirm or deny), and provide access to the information the school hold in accordance with the procedures laid down).

Publication Scheme
North Newton School has adopted the Model Publication Scheme for Schools approved by the Information Commissioner.

The Publication Scheme is published on our website and the materials it covers will be readily available from the office.

Dealing with Requests
The school will respond to all requests in accordance with the procedures laid down. The school will ensure that all staff are aware of the procedures.

Exemptions
The school will consider if information requested is subject to exemption. When the school wishes to apply a qualified exemption to a request, it will invoke the public interest test procedures to determine if public interest in applying the exemption outweighs the public interest in disclosing the information.

The school will maintain a register of requests where we have refused to supply information, and the reasons for the refusal. The register will be retained for 5 years.

Public Interest Test
The school will apply the Public Interest Test before any qualified exemptions are applied. Unless it is in the public interest to withhold information, it will be released.

Charging
The school will respond to most requests free of charge, and only charge where significant costs are incurred. The school may choose to charge a fee for complying with requests for information under FOI. The fees will be calculated according to FoI regulations and the person notified of the charge before information is supplied.

The school reserve the right to refuse to supply information where the cost of doing so exceeds the statutory maximum.

Responsibilities
The Governing body has delegated the day-to-day responsibility for compliance with the FoI to the Head Teacher. The Headteacher has nominated the Business Manager as the delegated person to deal with all FoI requests.

Complaints
Any comments or complaints will be dealt with through the school's normal complaints procedure. The school will maintain records of all complaints and their outcome.

If on investigation the school's original decision is upheld, then the school has a duty to inform the complainant of their right to appeal to the Information Commissioner's office.

FOI/EIR Complaints Resolution
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Who we are and what we do

Information to be Published	How the Information can be obtained (hard copy and/or website)	Cost
Who's who in the school	Hard copy: Prospectus/website	Cost of photocopies – see Schedule of charges, page 9
Who's who on the Governing Body and the basis of their appointment	Hard copy from School Office/website	
Instrument of Government	Hard copy from School Office	
Contact details for the Headteacher and for the Governing Body (named contact where possible with telephone number and email address (if used))	Hard copy from School Office	
School prospectus	Hard copy from School Office/website	
Staffing structure	Hard copy from School Office/website	
School session times and term dates	Hard copy: Prospectus/website	

What We Spend And How We Spend It

Information to be Published	How the Information can be obtained (hard copy and/or website)	Cost
Annual budget plan and financial statements	Hard copy from School Office	Cost of photocopies – see Schedule of charges, page 9
Capital funding	Hard copy from School Office	
Financial audit reports	Hard copy from School Office	
Details of expenditure items over £2000		
Procurement and contracts the school has entered into	Hard copy from School Office	
Pay policy	Hard copy from SCC	
Staff allowances and expenses that can be incurred or claimed, with totals paid to individual senior staff members	Hard copy from School Office	
Governors' allowances that can be incurred or claimed and a record of total payments made to individual governors	Hard copy of policy from School Office	

What Our Priorities Are And How We Are Doing

Information to be Published	How the Information can be obtained (hard copy and/or website)	Cost
School profile:		
• Performance data supplied by the government	Website	6p per B&W photocopy
• The latest Ofsted report	Website	
– Summary	Website	
– Full report	Hard copy from School Office	Cost of photocopies – see Schedule of charges, page 9
Performance management policy and procedures adopted by the Governing Body	Hard copy from School Office	
School's future plans	School Development Plan from School Office/website	
Safeguarding and child protection	Hard copy from School Office	

How We Make Decisions

Information to be Published	How the Information can be obtained (hard copy and/or website)	Cost
Admissions policy/decisions	Hard copy: Prospectus/website	Cost of photocopies – see Schedule of charges, page 9
Agendas and Minutes of meetings of the Governing Body and its committees	Hard copy from School Office	

Our Policies And Procedures

Information to be Published	How the Information can be obtained (hard copy and/or website)	Cost
School policies including:		
• Charging and remissions policy	Finance Policy hard copy from School Office/Website	
• Complaints procedure		
• Health and Safety	Hard copy from School Office/website	Cost of photocopies – see Schedule of charges, page 9
• Staff conduct	Hard copy from School Office	
• Discipline and grievance	Hard copy from School Office/website	
• Staffing Structure implementation plan	Hard copy from School Office/website	
• Information request handling		
Pupil and curriculum policies, including:		Cost of photocopies –
• Curriculum		see Schedule of charges, page 9
• Sex Education		
• Collective Worship		
• Pupil Discipline		
• Race Equality		
• Accessibility		
• Special Educational Needs	Hard copy from School Office/Website	Cost of photocopies – see Schedule of charges, page 9
Records management and personal data policies, including:		Cost of photocopies – see Schedule of charges, page 9
• Information security policies	Hard copy from School Office/Website	
• Records retention destruction and archive policies	Hard copy from School Office/Website	
• Data protection (inc. information sharing policies)		
• Policies and procedures for the recruitment of staff		

Lists And Registers

Information to be Published	How the Information can be obtained (hard copy and/or website – some information may only be available by inspection)	Cost
Disclosure logs	Single Central Record from School Office	Cost of photocopies – see Schedule of charges, page 9
Curriculum circulars and statutory instruments	Meet with head teacher to discuss request and format of reply	
Asset register	Inventory from School Office	
Any information the school is currently legally required to hold in publicly available registers	Meet with head teacher to discuss request and format of reply	

The Services We Offer

Information to be Published	How the Information can be obtained (hard copy and/or website – some information may only be available by inspection)	Cost
Extra-curricular activities	Hard copy from School Office/Website	Cost of photocopies – see Schedule of charges, page 9
Early Birds Breakfast Club	Hard copy from School Office/Website	
Services for which the school is entitled to recover a fee, together with those fees		
School publications	Hard copy from School Office	
Leaflets books and newsletters	Hard copy from School Office/Website	

Schedule Of Charges

This describes how the charges have been arrived at and should be published as part of the guide.

Type of Charge	Description	Basis of Charge
Disbursement Cost	Photocopying/printing @ 6p per sheet (black and white)	Actual cost per photocopy
	Photocopying/printing @ 10p per sheet (colour)	Actual cost per photocopy
	Postage	Actual cost of Royal Mail standard 2nd class
Statutory Fee	NIL	

DATA PROTECTION POLICY

Introduction
The School needs to keep certain information about our pupils, staff and other users to allow us, for example to monitor performance/achievement, Human Resource or safeguarding reasons.

The school will comply with the Data Protection Principles which are set out in the Data Protection Act 1998[1].

The Data Controller and the Designated Data Controllers
The School, as a body, is the Data Controller, and the Governors are therefore ultimately responsible for implementation.

The School has identified its Designated Data Controllers who will deal with day to day matters as: The Headteacher, Deputy Headteacher, and the senior administrator.

Responsibilities of the School
The school is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. This implies that:

a) all systems that involve personal data or confidential information will be examined to see that they meet the Data Protection Principles and Information Security guidelines
b) the school will inform all users about their rights regarding data protection
c) the school will provide training to ensure that staff know their responsibilities
d) the school will monitor its Data Protection and information security processes on a regular basis, changing practices if necessary.

Responsibilities of Staff
All staff are responsible for checking that any information that they provide to the School in connection with their employment is accurate and up to date.

All staff are also responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others when being used
b) is kept securely in a locked filing cabinet or drawer when not being used
c) be password protected both on a local hard drive and on a network drive that is regularly backed up
d) if kept on a laptop, usb memory sticks or other removable storage media, is password protected and encrypted. The device must be kept in a locked filing cabinet, drawer, or safe when not in use. The data held on these devices must be backed up regularly
e) is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure or transgression of the above statements will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Responsibilities of Parents/Guardians
The school will inform the Parents/Guardians of the importance and how to make any changes to personal data. This includes an annual data collection sheet which will be issued annually and the collection recorded.

Other permissions will also be sought in regards to matters such as the use of images and use of names in publicity materials on induction, annually or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

Rights to Access Information
All staff, parents and other users are entitled to:

a) know what information the School holds and processes about them
b) know how to gain access to view the data
c) know how to keep it up to date
d) know what the School is doing to comply with its obligations under the Act.

The School will place on its website a Fair Processing/Privacy Notice regarding the personal data held about them and the reasons for which it is processed.

All staff, parents and other users have a right to ask to view personal data being kept about them or their child. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher.

The School aims to comply with requests for access to personal information as quickly as possible and in compliance with advice from the Information Commissioner's Office and other professional agencies. They may be an administration charge which will be stated once the enquiry is made.

There is a separate policy for the processing of Freedom of Information requests.

Reporting incidents
Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Head Teacher, in the first instance.

SCHOOL COMPUTING POLICY

Introduction:
This policy expresses the school's purpose for the teaching and learning of Computing. It sets out the aims; planning of the curriculum and assessment and monitoring. It was developed in the autumn term) through discussion with teachers and the leadership team and based on Computing programmes of study (POS): key stages 1 and 2 (*DfE September 2014*).

Purpose:
We believe that an engaging and motivating Computing curriculum will enable our learners to:

- Use computational thinking and creativity to understand and change the world.
- Make deep links with mathematics, science and design and technology.
- Build knowledge of principles of information and computation, how digital systems work, and how to put this knowledge to use through programming.
- Become digitally literate – able to use, express themselves and develop ideas through information and communication technology.

Aims:

- The Computing Subject Leader and leadership team support staff to deliver a high quality computing education.
- Computational thinking – the ability to solve problems in a creative, logical and collaborative way – is developed through repeated programming opportunities and opportunities to build understanding and apply the concepts of computer science.
- Pupils become responsible, competent, confident and creative users of information and communication technology.
- Pupils have a growing awareness of how technology is used in the world around them and of the benefits that it provides. They are supported to evaluate and use information technology, including new or unfamiliar technologies.
- Opportunities for communication and collaboration develop understanding of the purposes for using technology and these are used to bring together home and school learning experiences.
- Technology is used imaginatively to engage all learners and widen their learning opportunities,
- Pupils have access to a variety of devices and resources and are encouraged to reflect on the choices they make to use them.
- We expect our pupils to:
    - Develop computing skills, knowledge and understanding
    - Develop an understanding of the wider applications of computer systems and communication technology in society
    - Develop independent and logical thinking through reasoning, decision making and problem solving
    - Develop imagination and creativity
    - Work independently and collaboratively

Curriculum coverage and progression:

- Planning for Computing is implemented using two core documents: the National Curriculum Programme of Study for Computing and the Statutory Framework for Early Years Foundation Stage
- Long term planning has been developed using the Somerset eLIM Computing Progressions and demonstrates coverage and progression of the attainment expectations at the end of Key Stage 1 and Key Stage as identified in the Computing POS.
- Medium term planning takes account of differentiation and progression and is based on Somerset progressions in Programming, e-safety, Multimedia, Handling Data and Technology in our Lives.
- The computer science aspects of Computing are taught discretely through the Programming and Technology in our Lives threads of Somerset's computing model.
- Key skills in information technology are developed through Multimedia and Handling Data threads and are integrated into learning in other curriculum areas.
- E-safety is developed through PSHE and, together with the threads of Technology in our Lives and Multimedia, builds the skills and understanding of Digital Literacy.
- Opportunities for technology as a tool to support learning and teaching in all areas are identified in curriculum planning.

Assessment:

- Progress is assessed on an on-going basis using the Somerset 'I can' statements for each thread of Computing. This ensures teachers are aware of individual pupil's progress in computer science, information technology and digital literacy.
- Formative assessment is used by the class teacher and teaching assistant during whole class or group teaching. Children's confidence and difficulties are observed and use to inform future planning.
- Each class teacher maintains a record, indicating pupils that are working beyond or below age-expected attainment. This is passed on to the next class teacher.
- Children are aware of the 'I can' statements and are encouraged to set success criteria for their work.
- Open questions are used to challenge children's thinking and learning.
- Children are encouraged to evaluate their own and others' work in a positive and supportive environment, including peer assessment.
- Teacher's judgments are supported through an electronic portfolio of evidence which provides examples of age-expected attainment.
- Information is shared with the school community through the school website, display, celebration events, newsletters, and end of year reports.

Early Years:

- Pupils build confidence to use technology purposefully to support their learning for all Early Learning Goals as appropriate.
- Pupils in Foundation Stage class will have experiences using technology indoors, outdoors and through role play in both child-initiated and teacher-directed time.
- The Foundation Stage teacher uses the Somerset Continuous provision map to plan for technology in a range of contexts.

Online safety:

- A progressive online safety curriculum ensures that all pupils are able to develop skills to keep them safe online.
- Opportunities for learning about online safety are part of PSHE and reinforced whenever technology is used.
- Clear rules for online safety are agreed by each class at the beginning of every year. Parents and pupils sign an acceptable user policy together when a pupil first starts at the school. The class rules are then signed annually by pupils and shared with parents.
- The Somerset BYTE scheme is used to ensure progression and coverage; and provides positive rewards for responsible use of technology.
- The school supports the international Safer Internet Day each February and provides opportunities for pupils to consider online bullying as part of Anti-Bullying week in the autumn term.
- Opportunities are taken whenever possible to reinforce messages of a healthy life style.
- The school has an online safety policy in place that details how the principles of online safety will be promoted and monitored.

Monitoring:

- The impact of the Computing curriculum is monitored regularly by the Computing subject leader through pupil discussion, samples of work and discussion with teachers, an electronic portfolio and the use of the NAACE Self Review Framework.
- Systematic monitoring of all threads of Computing informs the subject leader and school development plan.
- The Computing leader conducts regular audits of the training needs of teachers and teaching assistants to improve their subject knowledge and confidence. Requests for training in Computing can be part of individual teacher's performance management plan.

Equal opportunities:

- The school maintains its policy of equal opportunities as appropriate for Computing.
- Computers and related technology are made available to all pupils regardless of gender, race or abilities.
- The class teacher differentiates work by task, resource or support, to ensure the individual needs of more able and SEN pupils are met.
- The school is aware that not all pupils have the same access to computers at home and this is considered by staff in the planning and delivery of the curriculum.

Resources:

- The school has a range of resources to support the delivery of the Computing curriculum, the Early Years Framework and learning across all areas of the National curriculum. We maintain a list of resources used in each phase.
- Online tools such as Purple Mash are part of the experience of pupils.
- The Computing subject leader keeps up to date with new technologies and reviews the school's provision, as well as maintaining the existing resources in partnership with the school's technology support provider.
- Hardware and software faults are logged by the class teacher in a file kept in the staff room.
- The Computing Action Plan expresses the school's priorities for future expenditure and is reviewed by the Computing subject leader, governors and senior management who consider its impact on all learning.
- Governors and senior management ensure that they achieve value for money by implementing the principles of best value in evaluating, planning, procuring and using technology.
- Old resources are disposed of in line with Somerset County Council's environmental disposal policy and the school's data protection policy where these are applicable.

Roles and responsibilities:

- The school community works together to ensure the implementation of the Computing policy.
- The subject leader is responsible for monitoring curriculum coverage and the impact of learning and teaching; and assists colleagues in its implementation.
- Subject leaders in other curriculum areas are responsible for recognising the links between computing and English, Mathematics, Science and foundation subjects; and planning to use these to support learning across the school.
- Governors may include Computing in their learning walks around the school.
- The class teacher is responsible for delivering an effective Computing curriculum and integrating this into their planning for other subject areas where this is appropriate.
- The school receives technical support from Amy Brittan and the technician is responsible for the maintenance of computers, printers, the school network and keeping software up to date. The subject leader liaises with the technician to ensure that the systems are running efficiently.

- Age appropriate class and safety rules are displayed in the learning environment.
- Equipment is maintained to meet agreed safety standards.
- From Foundation Stage, pupils are taught to respect and care for technology equipment.
- Further guidance can be found in the school's health and safety policy.

PRIVACY NOTICE – DATA PROTECTION ACT 1998

We, North Newton Community Primary School, are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact Mrs. Hodge in the School Office.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following website:
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access this website we can send you a copy of this information. Please contact the LA or DfE as follows:

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Staff and Volunteer Acceptable Use Policy

School Policy
This Acceptable Use Policy reflects the school online policy.The school will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy
This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of school technology systems, school related use of technology systems outside of school, and make use of social networks personally and professionally.

My Responsibilities
I agree to:

- read, understand, sign and act in accordance with the School online safety policy
- report any suspected misuse or concerns to the Online Safety Leader
- monitor technology activity in lessons, extracurricular and extended school activities
- model the safe use of technology
- demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks making sure that these are in line with school ethos and policies especially at the time of a Critical Incident

Education
I agree to:

- provide age appropriate online safety learning opportunities as part of a progressive online safety curriculum
- respect copyright and educate the pupils to respect it as well

Training
I agree to:

- participate in online safety training
- request training if I identify an opportunity to improve on my professional abilities

Online bullying
I agree to:

- ensure the school's zero tolerance of bullying. In this context online bullying is seen as no different to other types of bullying.
- report any incidents of bullying in accordance with school procedures.

Sexting

- I will secure and switch off any device discovered with an intimate sexting image and report immediately to the safeguarding lead.
- I will not investigate, delete or resend the image.

Prevent

- I will continually develop children's ability to evaluate information accessed online.
- I will follow the agreed reporting procedure where children are purposefully searching for inappropriate sites or inadvertently accessing inappropriate sites.

Technical Infrastructure
I understand that the school will monitor my use of computers and the internet. I will not try to by-pass any of the technical security measures that have been put in place by the school which include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)

Security

- I will keep my password private and change it regularly.
- I will never log another user onto the system using my login
- I will lock (using Control/Alt/Del) my PC/laptop when away from my machine.

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 computer unsupervised
- I will report any filtering issues immediately

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.
- If I believe there has been a loss of personal or sensitive data, I will immediately report it to the Data Protection officer in the school.

Use of digital images

- I will follow the school's policy on using digital images especially in making sure that only those pupils whose parental permission has been given are published.
- I will not use personal devices for taking or sharing digital images within school without the direct permission of the Headteacher. Where permission has been given, I will ensure that all digital images relating to school are removed from my personal device at the earliest opportunity.

Communication

- I will be professional in all my communications and actions when using school ICT systems.
- I understand that I need to be open and transparent in all my communications.

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).

Social Media and Personal Publishing

- I will ask permission before I use social media with pupils or for other school related work.
- I will check with the SLT before I use sites/apps with learners to ensure that any pupil personal data is being held securely.
- I will follow the online policy concerning the personal use of social media.
- On any personal accounts I will not post any comments about any pupil and not post disparaging remarks about my employer/colleagues.
- When there is a Critical Incident I will not post any comments online.

Mobile Phones

- I will not use my personal mobile phone during contact time with pupils.
- I will not use my personal mobile phone to contact pupils or parents.

Reporting incidents

- I will report any incidents relating to online to the online Leader.
- I will make a note of any incidents in accordance with school procedures.
- 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 pupils 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/VOLUNTEER ACCEPTABLE USE/ONLINE POLICY

I have read and understand the full School online policy and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name _____

Signed _____

Date _____

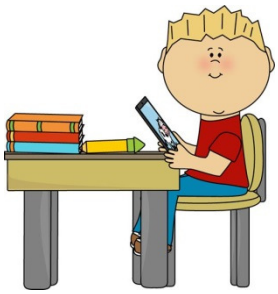
NORTH NEWTON COMMUNITY PRIMARY SCHOOL
"TOGETHER WE ACHIEVE"

Acceptable Use Policy Agreement for Key Stage 1

Child's Name:

.....

This is how we stay safe when we use computers:



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

Signed …….. Parent

Date ……..

Ref: Forms\Consent\KS1 Acceptable Use Agreement

NORTH NEWTON COMMUNITY PRIMARY SCHOOL

KS2 PUPIL ACCEPTABLE USE AGREEMENT

Technology is a great tool to find information and to communicate with others.

The School encourages appropriate, effective and safe use.

Users of technology must agree to certain rules and will only use equipment and software as instructed.

My Responsibilities:

- I will act responsibly when using technology, computers or the internet.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line at home or in school.
- I will not disclose or share personal information about myself or others when on-line.
- I will report any suspected misuse or problems to a teacher or adult immediately.
- I will make sure I have permission to use any material that I find.

Cyberbullying:

- 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 cannot be mistaken as bullying.
- I understand that I should report any incidents of bullying.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

Access to Internet Sites

- I will not try to access sites that are blocked or that are unsuitable for use in school.

Communication – email, social networks, blog, etc.:

- I will be careful in my communications making sure that nothing I write is offensive.
- I will not write anything that could be seen as insulting to the school, someone or something else.

Sanctions:

- I understand that there are regulations in place when pupils use technology and there are sanctions if I do not follow the rules.

Pupil Acceptable Use Agreement Form

Please sign to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the Agreement and agree to follow these guidelines when I use the school ICT systems and equipment (both in and out of school).

Blogging: From time to time I will be involved in blogging activities and agree to follow the class rules.

Name of Pupil ……

Class……

Signed ……

Date ……

MONITORING

This policy will be reviewed annually.

Signed …… Chair of Governors

Date ……