Cleadon Church of England Academy

Communications Network
E-Safety Policy

(Reviewed April 2016)

Policy Reviewed and Adopted by Governing Body:
Approved:
Date of Next Review: Summer 2019

School Policy Statement

Believe

Inspire

Excel

Mission Statement

Guided by our caring Christian ethos, we all work together to equip everyone with the skills, attitude, creativity and motivation to become happy successful lifelong learners and respectful global citizens.

Values	
We will bring our Christian ethos to life by:	
Striving for excellence	• Setting high expectations, • Showing pride, passion and self-belief, • Encouraging forward thinking and embracing challenge, • Promoting continuous learning, • Recruiting the right people, • Facilitating continuous improvement, • Providing the widest range of opportunities to excel.
Achieving together	• Learning and working together harmoniously, within a supportive environment, • Ensuring everyone is valued, • Enabling everyone to have a voice, • Promoting shared understanding and ownership, through collaboration, • Sharing good practice, and celebrating success, • Challenging ourselves and others, • Supporting the communities in which we live and work.
Showing respect	• Promoting the wellbeing of all members, • Recognizing everybody's contribution, • Demonstrating courtesy and fairness to all, • Embracing diversity and practicing tolerance, • Celebrating the individual.
Inspiring success	• Nurturing achievement and celebrating success, • Embracing inspiration and innovation, • Encouraging self-motivation, • Providing inspirational, creative teaching and challenge, • Providing positive role models, • Delivering a broad and exciting curriculum that engages and enthuses all learners.
Acting with integrity	• Maintaining professionalism at all times, • Valuing honesty, trust and accepting accountability, • Establishing transparent and effective communication, • Listening and acting upon feedback, • Ensuring collective care and responsibility.
This will be delivered within a caring, happy, safe and secure environment.	

Philosophy and Culture

The school encourages the use creatively and safely a wide range of innovative and integrated broadband technologies, together with the development of appropriate skills to analyze and evaluate these resources. The school will promote high standards of teaching and learning by supporting the effective use of ICT and provide a safe Environment, respect for all, non tolerance of bullying.

Equal Opportunities

All pupils regardless of ability, gender or race are entitled to and will receive access to broadband technologies through the internet and its resources throughout the school.

Roles and Responsibilities in Relation to Internet

Our school uses Northern Grid for Learning's Network and BT Service to access the broadband internet. We are required to comply with the NGFL's Acceptable Use Policy (AUP) which must be signed and agreed by the School Principal.

All adult users of the school network and internet must read and understand the scope of this E-safety policy and then sign an Acceptable use agreement before being allowed access to the school services.

All Pupil users will sign and agree to acceptable user rules and procedures appropriate to their age and understanding.

Monitoring and Reporting

This e-safety policy was approved by the Board of Directors on:	April 2016
The implementation of this e-safety policy will be monitored by:	School Principal (Mrs. J. Gray) Subject Leader (Mrs C Dowson)
Monitoring will take place at regular intervals:	Annually
Reporting to the Board of Directors at regular intervals:	Annually
The E-safety policy will be reviewed annually or more regularly in the light of new developments in the use of technologies, threats to e-safety or incidents that have taken place. The next review date will be:	October 2015
Should serious e-safety incidents take place the following external persons/agencies should be informed:	Internet activity reports to the Principal then appropriate authorities to be informed of any serious e-safety incidents.

The school will monitor the use of the policy using:

- Logs of reported incidents
- Northern Grid and LA monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys/questionnaires

Reporting Accidental or Illegal Access

It is impossible to guarantee that there will never be accidental or illegal access to inappropriate or offensive material. Should a user of the Cleadon Domain Network access a site that they deem to be inappropriate by accident should do the following:

- Inform the school's Principal and E-Safety officer of the incident and give the website address.

- Pupils should activate screening software immediately (Hector Protector).

- The site will be recorded in the e-safety log and filtering adjusted if necessary. Do not show anyone the content or make public the URL. If reporting a URL do not copy and paste, type the address.

- Go to the IWF website at www.iwf.gov.uk and click the report button.

- The school's E-Safety officer should ring the Open Zone and LEA school support helpdesk – tel. no 0845 333 4568 and report the web address asking for an investigation as to whether the website should be permanently blocked.

- If LEA decide that the website is not sufficiently inappropriate for permanent blocking, the school should block the website via its own Cache Pilot or other proxy server.

Reporting Deliberate Abuse or Misuse

Users must report and a log made of all e-safety concerns such as deliberate access to inappropriate sites, unacceptable e-mail and any instances of cyber bullying. The report will be made to the E-Safety Officer who will then decide whether the incident should be progressed further in accordance with guidance issued by the LA. If necessary the following actions would take place:

- The Local Authority should complete an internal RIPA form, requiring Cleadon Church of England Academy to complete an internal investigation.

- If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, the school will inform the relevant police authority who will complete their own investigations.

- If the investigation confirms that inappropriate behaviour has occurred, Cleadon Church of England Academy will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.

- In the event of suspected misuse and image of the hard drive should be created using disc imaging software such as Acronis or Norton Ghost.

Sanctions for Misuse

Cleadon Church of England Academy wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its users. The school system is monitored on a regular basis and any misuse is reported and followed through.

In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow. The school will also assist where necessary should an investigation be called for by the police.

In other instances the user may be restricted from using the service for a period determined by the school Principal. Disciplinary action may also be taken.

All cases of inappropriate use are logged in the E-Safety Log, held in the Office. All cases of sites deemed inappropriate by the school and the action taken are also held on file.

Unlawful or Illegal Use

Cleadon Domain Network users agree to use the service for lawful purposes only and not to use the Service to send or receive materials or data, which is:

- in violation of any law or regulation

- which is defamatory, offensive, abusive, indecent, obscene

- which constitutes harassment

- is in breach of confidence, privacy, trade secrets

- is in breach of any third party Intellectual Property rights (including copyright)

- is in breach of any other rights or has any fraudulent purpose of effect.

Cleadon Domain Network users are prohibited from storing, distributing or transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through the Service.
Examples of unlawful material include:

- direct threats of physical harm

- hard core and child abuse images

- copyrighted, trademarked and other proprietary material used without proper authorisation

Cleadon Domain Network users may not post, upload or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on our servers without the consent of the copyright holder. Cleadon Domain Network users must give acknowledgement to the source wherever such material is used.

In the event that the school, NGFL or BT become aware of any breach of this clause, action may be taken. The storage, distribution, or transmission of unlawful materials could also lead to UK authorities alleging criminal liability.

Cleadon Domain Network users ***should be aware that disciplinary and/or civil action might arise if users are found to be accessing material of this nature across the school, Local Authority or regional network.***

Security and Protection

All users of the Cleadon Domain Network are required to be individually identifiable:

- Every user of the network must have an individual username and password. This must be securely kept and not passed onto other users.

- All wireless networks in use must be secure to ensure no other outside wireless networks can access the schools system.

Those members of staff who have administration rights to their school network should take care to ensure that no unauthorised user obtains access to their admin password:

- This includes accidental or deliberate access by leaving admin machines active when not in use by authorised personnel.

- We must not connect to the network any unprotected machine, insecure proxy servers, or other machines vulnerable to unauthorised remote access giving unknown attackers access at either user or administrator level.

In the event of an investigation into misuse, proper use of passwords will protect innocent users from the upset and embarrassment of suspicion for inappropriate or illegal misuse.

Violations of System or Network Security

Any violations of systems or network security are prohibited, and may result in the user facing criminal and civil liability. Cleadon Church of England Academy and Northern Grid will investigate incidents involving such violations and will inform and co-operate with the relevant law enforcement organisations if a criminal violation is suspected. The user may be refused access to the network as a result of any breach of security.
Violations may include, but are not limited to, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network

- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network

- Interfering with any user, host or network including mail-bombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

All machines connected to the Northern Grid network must have full up to date and appropriate virus protection. No user should try to remove or alter this software. Any violation will mean immediate removal of access.

No machine should be connected to the internet without protection. Any machine found to be infecting the Local Area Network (LAN) must be immediately disconnected, cleaned and not reconnected to the LAN until fully checked by an authorised school officer.

All users must log in to the school LAN and use the Northern Grid network to access the internet. No other method of access is permitted.

Any violations of systems or network security are prohibited, and will be investigated which may result in the user facing criminal and civil action.

Email Use

At Cleadon Church of England Academy users must use the e-mail address issued by the school for employment purposes only.

Cleadon Domain Network users may not send e-mail to any user who does not wish to receive it. Users must refrain from sending further e-mail to a user after receiving a request to stop.

Chain letters, flood e-mails and mail bombs may not be propagated using the Service. Cleadon Domain Network users may not operate or assist in any way whatsoever any web site, email address, email service, ftp service or any other online service, which is advertised or promoted by means of Unsolicited Bulk Email

Cleadon Domain Network users may not use false e-mail headers or alter the headers of e-mail messages to conceal their e-mail address or to prevent Internet users from responding to messages. Cleadon Domain Network users may not use any email address that you are not authorised to use.

E-mail sent through the school service is deemed to be representing the school. As such any e-mail must not contain defamatory remarks, offensive language or other inappropriate material.

Attachments may only be opened if you are certain they do not contain any virus or other damaging content.

All users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

World Wide Web Usage

At Cleadon Church of England Academy all access to the Internet is filtered via a Cachepilot or a similar proxy server.

The school monitors internet sites visited and may prohibit access to some sites deemed unacceptable or inappropriate.

All Internet usage from the Northern Grid network is monitored and logged and a log is kept of all sites visited. When specific circumstances of abuse warrant it, individual web sessions will be investigated and traced to the relevant site and user account. Such an investigation may result in action and possibly criminal investigation.

Copyright and Plagiarism

It is understood that:

- Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

- The laws of all nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities.

- Documents or material must not be published or accessed on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Images

It is understood that:

Any images that involve children must not identify children by name and permission must have been agreed by the child and/or relevant parent /carer before posting.
A record should be made of who will be taking the photos, why the photos are being taken, when they are being taken and what they are to be used for.
This should all be documented in the risk assessment carried out before a school trip or event.
The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Principal.

- Any images from cameras memory cards or mobile devices must be downloaded to a LAN secure shared area and store in a clearly labelled folder. This must be done within seven days.

- Delete original images on camera or other device prior to it being taken off site.

- Before using images in other media (eg email, online, paper based and other collateral) ensure permission given covers intended use.

- Equipment must not be available for further use until images have been transferred/deleted.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg: on social networking sites.

- All staff will make every effort to use school equipment when taking images, however the use of personal devices is deemed to be acceptable provided that the images are transferred/deleted from the device at the earliest opportunity when returning to school and not later than 7 days after the images were taken.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Uploading material

It is understood that:

Permission will be obtained before uploading video or photos on the internet. Pupils uploading material will be moderated by a teacher before posting. All users must remember that posted material represents the school and should not bring the school into disrepute.

Video Conferencing & Skyping

The Cleadon Domain Network facilitates effective video conferencing & Skyping. As educational tools, these systems have many benefits. However, to ensure effective safety we are recommended to use the following:

- Always book the VC session via the national JVCS booking system. This ensures that you will be connected to the correct end user and that the session is monitored.
    - JANET Number- cleadon-ce-primary-school@s-tyneside-mbc.gov.uk
    - E164 Number – 0044021021   Phone Number-3316200

- Always use VC and Skype in a public place. Only carried out with a member of staff present. Pupils or young people must not be unattended during a live VC or Skype event.

- Report any misuse of VC or Skype to your school E-Safety officer and to the Northern Grid for Learning.

Mobile Devices

Cleadon Church of England Academy does not prohibit the use of mobile devices on the regional network. However, users should note the following items. These examples are for clarification. They are not exclusive:

- Mobile devices such as phones, PDA's, PSP's, E-books, web books, MP3 players, Nintendo DS, flash drives, portable hard drives and laptops may be used in school for educational purposes. Users must follow the guidance for connecting to the school network and accessing the internet.

- Any of the above mobile devices must not be used to take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission.

- Pupils may only send and receive files using portable devices, Bluetooth or the internet under supervision of the teacher and as part of their education. Pupils who bring personal mobile devices into school will be required to follow health and safety guidelines and give the device to a member of staff for safekeeping.

- Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

- Staff may use personal portable devices to further their teaching responsibilities during directed time. Staff should ensure that Bluetooth is turned off or hidden and that private use of mobile technologies is carried out in a responsible manner. Staff should ensure that Bluetooth names are appropriate for educational settings.

- Any mobile device must be checked for viruses and spam content before being attached to the regional broadband network.

Passwords

At Cleadon Church of England Academy all users must log in to the school LAN and the internet using user name and password provided. These must be kept secure, and no-one should give their user details to another to use. Any limitations in log in should be notified to the network administrator immediately. Breach may mean access is denied. Even the youngest pupils should be encouraged to have individual user names and passwords appropriate to their age.

Visitors to the Cleadon Network Domain will also be given a user name and password. These will be rescinded when the visitor leaves. Any files or documents will be kept for a short while, up to 3 months, and then deleted from the system.

Any users taking part in parent courses will have access to shared area monitored by the tutor.

Any access to the LAN will be granted at various levels deemed appropriate to the level of need of the user, ie: pupils, governors and parents will have differing needs and access levels to staff.

Higher access levels are granted to administrator and technician.

Any work conducted on the Cleadon Network Domain must be supervised by technician, administrator or agent of the NGFL or LEA. All software must be installed by an authorised person or their agent.

Users should not share logins or passwords. Passwords should be changed regularly.

All passwords should be complex in nature including capitals, lowercase, symbols and numerals. The more complex the password the more protection you are providing. Passwords should be between 8-10 characters using single letters. A phrase password, which includes spaces, may be easier to remember.

All machines should be locked or logged out when unattended. Staff should also follow the policy of the school for security of the premises and equipment on it.

Pupils or Staff Leaving the School Network

At Cleadon Church of England Academy logins will be cancelled within 1 week. Files should be transferred to the new teacher/school if appropriate. Files will be stored for a short while, 3 months, then deleted.

Learning platform account and e mail will be disabled within 1 week. The account will not be deleted so as useful documents can still be utilised by the school.

- Portable devices need to be thoroughly checked for inappropriate content, malware, illegal copies etc. prior to being made available to other users.

- Files, programs, data - ensure none are taken away from the school if the copyright is only for the institution.

- Images – no teacher can take images of pupils away from the school when they cease to be employed by the school.

- 'Shared Accounts –change any shared service passwords such as administrator accounts on servers, printers and network devices if necessary.

- Service contracts and web sites where the employee is a named contact will need to be updated.

Social Networking and Media

Cleadon Church of England Academy may use an e-mail distribution list to send messages to selected groups of users.

Staff will moderate collaboration tools such as newsgroups and chat rooms if used on the school network for learning purposes.

Students will be denied access to public or un-moderated chat rooms.

Staff will moderate social media tools such as blogs and wiki's if used on the school network for learning purposes.

Staff should follow the guidance set out in the Staff handbook and Staff Acceptable Use policy with regard to Social Networking Sites.

Storage of Information

At Cleadon Church of England Academy digital images may only be stored on the LAN in recognized files. (See Images) These will be detailed with date and title of school event. Should users need to store images in local document folders these will be kept to a minimum and kept public.

No images will be stored in private or password protected areas of the network.

School images stored on teacher laptops will also be in an identifiable folder clearly visible on the desktop. Images will be kept for teaching purposes only. Any publication of images will conform to the school policy. Individuals will not be identifiable by name or year group unless parental permission is obtained. Work may be identified by Christian name and year group only, however it should preferably remain anonymous.

Data files, resources and planning files will be stored in clearly labeled folders and handed over if the member of staff leaves. Storage of pupil information follows guidance in the data protection act. Files may be transferred on USB sticks only if the USB stick has been encrypted. Files should be uploaded to named folders and not remain on USB sticks for more than 1 month.

Use of School Equipment

At Cleadon Church of England Academy school laptops and equipment should only be used by the nominated school employee and for educational use only.

E Safety Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating the pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT/Computing across the curriculum.

At Cleadon Church of England Academy E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT/Computing/PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.

- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Rules for use of ICT systems and internet will be posted in all rooms and displayed on log-on screens.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Parents and Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

Cleadon Church of England Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE

- Parent's evenings & Individual meetings.

- E-safety Workshops

Staff

It is essential that all staff at Cleadon Church of England Academy receive e-safety training and understand their responsibilities. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff through CPD. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Policies.

- The E-Safety Coordinator will receive regular updates through attendance at NGfl &LA conferences and other information and training sessions and by reviewing guidance documents released by Ofsted/NGfL /LA and others.

- This E-Safety policy and its updates will be presented to and discussed by staff in whole staff or team meetings and INSET days.

- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

Governors

Cleadon Church of England Academy Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of any group involved in ICT, E-Safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / NGfL or other relevant organisation.

- Participation in school training and information sessions for staff or parents.

Technical – Infrastructure / Equipment, Filtering and Monitoring

Cleadon Church of England Academy has a managed ICT service provided by South Tyneside Council, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the NGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.

- There will be regular reviews and audits of the safety and security of school ICT systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.

- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg school safe).

- (Alternatively, where the system allows more than one "master / administrator" log-on, the Principal or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access).

- Remote management tools are used by technical staff to control workstations and view users activity.

- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager, E Safety Officer (or other relevant person).

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

Cache Pilot

The following to be address and carried out termly by the school technician under the authority of the Principal:

1. Always have all machines authenticated and directed through the cache.
2. Set up lists of approved sites.

The Cache Pilot allows tailored URLs for individuals and groups

Appendix I

Relevant Legislation:

The following are a list of Acts that apply to the use of Northern Grid Network and Services:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Equality Act 2010
- Obscene Publications Act 1959 and 1964
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice and Public Order Act 1994
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- The Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Human Rights Act 1998
- Communications Act 2003
- Malicious Communications Act 1988
- Trade Marks Act 1994
- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Public Order Act 1986
- Education and Inspections Act 2006

References:

Byron Review – Children and New Technology – "Safer Children in a Digital World"
SWGfL
BECTA
Department for Education
Northern Grid for Learning (NGfl)
Wikipedia
Legislation.gov.uk
Websitelaw.co.uk

Northern Grid

The Northern Grid Network and Services are provided by Northern Grid for Learning, a company registered in England and Wales (company number 4824016) whose registered office is 11 Vance Business Park, Norwood Road, Gateshead, NE11 9NE.

Appendix 2

Communication Technologies Grid

Communication Technologies	Staff and other adults				Students/pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones or other camera devices								
Use of hand held devices eg PDAs, PSPs, Nintendo DSi								
Use of personal e mail addresses in school, or on school network								
Use of school e mail for personal e mails								
Use of chat rooms/facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								

Appendix 3

	User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					✓
	Promotion or conduct of illegal acts, eg: under the child protection, obscenity, computer misuse and fraud legislation					✓
	Adult material that potentially breaches the Obscene Publications Act in the UK					✓
	Criminally racist material in the UK					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Promotion of racial or religious hatred				✓	
	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 NGfL, South Tyneside LA and / or the school				✓	
	Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
	Revealing or publicising confidential or proprietary information (eg: financial / personal information, databases, computer / network				✓	

access codes and passwords)					
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non educational)		✓			
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Use of video broadcasting eg: Youtube			✓		

User Actions Grid

Appendix 4

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers/Principals, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Equality Act 2010

This Act consolidated the complicated and numerous array of Acts and Regulations, which formed the basis of anti-discrimination law in Great Britain. This was, primarily, the Equal Pay Act 1970, the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995 and three major statutory instruments protecting discrimination in employment on grounds of religion or belief, sexual orientation and age. This legislation has the same goals as the four major EU Equal Treatment Directives, whose provisions it mirrors and implements. It requires equal treatment in access to employment as well as private and public services, regardless of the protected characteristics of age, disability, gender reassignment, marriage and civil partnership, race, religion or belief, sex, and sexual orientation.

Patents Act 1977

This Act covers an invention or an inventive step. It is similar to copyright in that it gives the owner of the patent exclusive rights to prevent others from making, using, selling, or distributing the patented invention without permission.

Defamation Act 1996

Defamation is a false statement made by one individual about another. This statement attempts to discredit that person's character, reputation or credit worthiness. In order to be defamatory, such a statement must be communicated to at least one other person.

The Regulation of Investigatory Powers Act 2000

Also referred to as **RIPA.** This act is concerned with regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. It was introduced to take account of technological change such as the growth of the Internet and strong encryption. In a school situation this would be requested if you or the LA or another law enforcement agency contacted you with suspicions that the school network was being used for illegal purposes eg: gaining access to potentially illegal material e.g. Child abuse images, or is suspected of inappropriate Internet / email use.

Digital Economy Act 2010