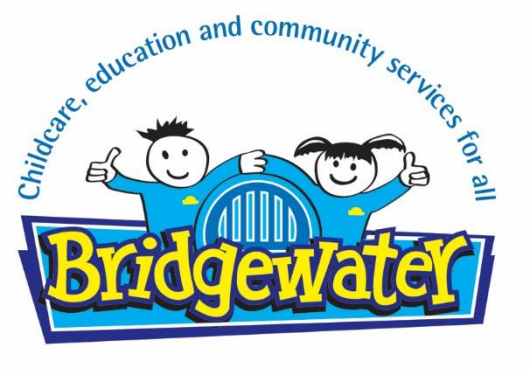
Online - Safety Policy



Contents

APPENDICES

1.0 Who will write and review the policy?

Issue date:	March 2018
Reviewed by:	Luke Moralee
Ratified by Governors:	
Reviewed on:	Spring 2025
Next review date:	Spring 2026

Senior Manager with responsibility for whole school ICT:	Business Manager
Computing Subject Leader:	Luke Moralee
Safeguarding Responsibility:	Sam Robson
Technician:	Newcastle City Council
Computing Governors:	Stuart Taylor/Shaz Khan

Monitoring of the Information and Communication Technology (ICT) policy is the responsibility of the ICT Team and Senior Management of the school.

The policy is reviewed each year by the ICT Team and Senior Leadership Team and fully revised and presented to Governors for final approval every three years before being issued to staff.

As Online safety is an important aspect of strategic leadership within the school, the Head teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online safety Coordinator in this school is the Business Manager who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the Online safety Coordinator to keep abreast of current issues and guidance through organisations such as Newcastle Local Authority, Department for Education, Child Exploitation and Online Protection Centre (CEOP), and Childnet.

Senior Management and Governors are updated by the Head teacher and Online safety Coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and children, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

- Child Protection
- Health and Safety
- Home - School Agreements
- Behaviour / Pupil Discipline (including the Anti-Bullying)
- PSHCE
- Corporate ICT Policies

- Use of AI in school

2.0 Teaching and Learning

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to world-wide educational resources, including museums and art galleries.
- Inclusion in the National Education Network (www.nen.gov.uk) which connects all UK schools.
- Educational and cultural exchanges between children world-wide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for children and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient.

Our aim is to produce learners who are confident and effective users of ICT. We strive to achieve this by:

- Helping all children to use ICT with purpose and enjoyment.
- Helping all children to develop the necessary skills to exploit ICT.
- Helping all children to become autonomous users of ICT.
- Helping all children to evaluate the benefits of ICT and its impact on society.
- Meeting the requirements of the National Curriculum and helping all children to achieve the highest possible standards of achievement.
- Using ICT to develop partnerships beyond the school.
- Developing computational thinking.
- Celebrating success in the use of ICT and Computing.

2.1 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. Computing skills and knowledge are vital to access life-long learning and employment; indeed, Computing is now seen as a functional,

essential life-skill alongside English and mathematics. The statutory curriculum requires children to learn how to locate, retrieve and exchange information using technology including the Internet. All Children should be taught to use the Internet and electronic devices efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhance the school's management information and business administration systems.

2.2 Education – Children

Online safety should be a focus in all areas of the curriculum and staff should reinforce Online safety messages across the curriculum. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key Online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be helped to understand the need for the Code of Conduct Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. In lessons, children are supported in how to report unsuitable material to an appropriate adult.
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Sites that are temporarily unblocked should be then blocked again once the research topic is complete.

2.3 Education – Parents / Carers

Many parents and carers have only a limited understanding of Online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, websites, Class Dojo, Seesaw
- Parents sessions, Parent's Evenings and Digital Parenting Magazine
- High profile events / campaigns e.g. Safer Internet Day
- Termly e-safety newsletters to parents shared via Classdojo

2.4 Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide Online safety information for the wider community, as well as the e-safety newsletter.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online safety provision where/when appropriate.

2.5 Education & Training – Staff / Volunteers

It is essential that all staff receive Online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online safety training needs of all staff will be carried out regularly.
- All new staff should receive Online safety training as part of their induction programme, ensuring that they fully understand the school Online safety policy and Acceptable Use Agreements.
- The Online safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Online safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.
- Information and training from Clennel Education Solutions.

2.6 Training – Governors

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

- Information and training from Clennel Education Solutions.
- Make Governors aware of possible participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

3.1 How will email be managed?

- Children may only use approved email accounts (Office 365 – accounts, directly linked to the child's username or, where appropriate Tocomail accounts set up and monitored by the Class Teacher)
- Children must immediately tell a teacher if they receive offensive email
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone
- Approved (Bridgewater issued) email addresses will be used for communication outside of the school
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper
- The forwarding of chain messages is not permitted
- Staff should not use personal email accounts during school hours or for professional purposes

3.2 School website

- The contact details on the website should be the school address, email and telephone number. Staff or children's personal information must not be published.
- The head teacher, delegated to the Business Manager, will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The school website should only show images of children whose parents have given written permission to do so.

3.3 Can Children images or work be published?

- Images that include children will be selected carefully and will not provide material that could be reused.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers must be obtained before images of children are electronically published.
- Children's work can only be published with their parent's permission, (see Appendix VII).

3.4 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice if classroom use is to be developed. The rapid rise of AI technology has meant that a separate 'Generative AI in school' policy has needed to be developed.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.5 Mobile Devices

This section sets out what is 'acceptable' and 'unacceptable' use of mobile devices by the whole school community (students, staff and visitors) while they are at School or undertaking school activities away from school.

Mobile devices are now a feature of modern society and every child in school has access to one. The technology of mobile devices has developed such that

they now have the facility to record sound, take photographs and video images and connect to the internet. Therefore, the school also recognises the advantages mobile devices have as a ubiquitous learning tool.

3.5.1 General issues

- Mobile Technology should only be used in School with the permission of a member of staff and in accordance with their instructions.
- Mobile devices brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- The school allows staff to bring in personal mobile phones and devices for their own use during non-contact rest periods only – these are to be used in restricted areas, eg. Staffroom, PPA room, Offices etc or with express permission of the Headteacher.
- During contact time, personal devices should be switched off and put away beyond use, apart from designated staff with a responsibility for Health & Safety and / or Safeguarding.
- Designated 'mobile use free' areas are situated across the setting. The areas which should be considered most vulnerable include: toilets, bathrooms and changing areas.
- School devices will only be used to take photos or videos, when appropriate, and only published where parental permission is in place.
- All visitors are requested to keep their phones on silent.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School office.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, these devices should only be used for school business (e.g. contacting parents, taking photographs and videos, tweeting and Facebook status updates).
- It is the responsibility of parents and children to ensure mobile devices are adequately insured.

3.5.2 Students use of mobile devices

- The school strongly advises that student mobile phones and devices should not be brought into school.
- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. On these occasions school must be informed in advance and the mobile phone handed to a member of staff on arrival at school.
- Any unauthorised device brought into school will be confiscated.
- The school cannot take responsibility for loss or damage to children's personal mobile technology. Devices should not be left unattended in school, e.g. in bags or table trays.
- Parents should be aware of the potential risks for children of using mobile technology such as theft, bullying and inappropriate contact, including grooming by unsuitable persons.
- Parents are encouraged to ensure that suitable tracking and filtering systems are activated on mobile technology used by their children.

3.5.3 Staff use of mobile devices

- Staff should ensure they cannot be distracted from their work with children. For example, phones should be turned off and put away beyond use.
- Personal mobile devices should not be used around children, in particular photographs and video should only be taken on school issued devices.
- It is essential that staff do not put themselves at risk of allegations.
- Images and video of children should never be taken without having secured signed permission from the parent or carer.
- School devices containing personal information, including photographs and video of children, should not be taken off the premises,

  a) except where parental permission has agreed to staff using photographs and video for assessment purposes.

  Or

  b) except with the explicit agreement of SLT in each and every case.

- Any images taken with permission are the property of the school and should only be used in relation to school business.
- Staff should never contact a pupil or parent / carer using their personal device.
- School owned devices for staff use should be secured with a pin code and should not be left unattended or on display. Any loss or theft of school

owned devices should be reported to the Head teacher or equivalent immediately.

- Staff will be provided handheld devices as the school deems necessary in order to deliver the majority of your role, personal devices should not be used as part of teaching and learning.
- Personal devices may be used for teaching activities, but should have all notifications (for emails etc.) shut off, to avoid personal information being shared and displayed accidentally with Children. Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox etc.).
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- "Malicious communication" between any members of the school community is not allowed, e.g. text messages or online chat.

Schools and settings should ensure that staff adhere to their "Acceptable Use Policy" – which should be signed by staff, children, governors and parents - and that common sense is used at all times.

3.5.4 Wearable Technology

Staff

If Wearable Tech is worn in lessons or in public areas around the school, the 'Do not disturb'/'flight mode' should be activated.

Children

Wearable Technology that has the ability to communicate, ie Camera, Microphone or message notifications, are not allowed to be worn in school. Children must seek permission from the school before wearing fitness tracking devices.

If a Wearable Tech device is deemed by the teacher to be causing a distraction around school, it is liable to confiscation until the end of the school day.

3.6 Laptops

- Staff provided with a laptop purchased by the school can only use it for private purposes at the discretion of the Head teacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the Computing subject leader.
- Laptops belonging to the school must have updated antivirus software installed and be password protected and encrypted.
- Staff provided with a laptop purchased by the school are responsible for updating the antivirus software by connecting to the school network regularly.
- Staff should ensure that their school laptops are regularly brought onto site so that they can be updated.
- Staff intending to bring personal laptops on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop.
- Staff should not attach personal laptops to the school network.
- The security of school laptops is of prime importance due to their portable nature and them being susceptible to theft.
- See School Laptop policy (separate document).

3.7 Social Media

- The school will not publish children's full names in association with any photographs uploaded to social media.
- Written permission from parents or carers must be obtained before images of children or their work are electronically published.
- The school encourages parents and carers to comment on posts appropriately, but are not responsible for comments or likes of uploaded content from the school account. However, the school will manage content within our control.
- The school will be unable to answer direct messages on social media. Questions or queries should be directed to the school office, as is normal practice.
- If a complaint is to be made about the content on social media, the official channels, as set out in the Complaints Procedure, should be followed.
- Staff or volunteers must not make comments on behalf of the school or claim to represent the views of the school, unless they have explicit permission from the Headteacher to do so.

- Staff or volunteers should be aware of the information and content available on their own social media feeds and take appropriate action to keep their details safe.

4.1 Internet access

- The school will maintain a current record of all staff and Children who are granted access to the school's computers and ICT equipment.
- All staff must read and sign the 'Acceptable use for staff agreement' before using any school Computing/ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific approved online materials.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that children will be provided with supervised Internet access (see Appendix II).

4.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material through the use of corporate filtering systems. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a computer connected to the school network. The school or Newcastle Local Authority does not accept liability for any material accessed, or any consequences resulting from Internet use.
- The final decision when assessing risks will rest with the Head teacher.

4.3 Handling Online safety complaints

- Complaints of ICT/Internet misuse must be recorded and will be dealt with by a senior member of staff, who will decide if sanctions are to be imposed.
- Any complaint about staff misuse must be referred to the Head teacher who will decide if sanctions are to be imposed.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- The Head teacher will arrange contact/ discussions with Newcastle Local Authority and the police to establish clear procedures for handling potentially illegal issues.

- Any complaint about illegal misuse must be referred to the Head teacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Newcastle Local Authority.
- All staff, children and parents will be informed of the complaints procedure.
- All staff, children and parents will be informed of the consequences of misusing the Internet and ICT equipment.

4.4 Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Anti-Bullying Policy.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of Cyberbullying reported to the school are recorded.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Children, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the origin of any cyberbullying, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyberbullying may include:

- The child will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/Carers will be informed.
- The police will be contacted if a criminal offence is suspected.

5.1 Sharing with Children

- Online safety rules and posters will be displayed in all rooms where computers are used and highlighted/discussed during ICT sessions.
- Children will be made aware that their network and Internet use will be monitored.

- An Online safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- An Online safety module is included in the Computing scheme of work and PSHE curriculum.

5.2 Sharing with staff

- Staff will be consulted when creating and reviewing the Online safety policy.
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook.
- Every member of staff, whether permanent, temporary or supply, will be informed that Network and Internet traffic will be monitored and can be traced, ensuring individual accountability.

5.2 Monitoring & Evaluation

- Pupil Voice completed by the children. For instance, those completed before and after online safety sessions, monitored by the Computing lead teacher.
- Anecdotal feedback from staff.
- Annual safety audit.
- Procedures will also be updated following Local Authority advice.

Code of Conduct for Children

I agree to follow these rules when using the Internet:

- I will not share my username, password or personal information with anyone else
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I will not look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this I will tell a teacher immediately
- I will only upload materials which are free from copyright and suitable for school use
- I will not deliberately misuse or deface other users' work on the school network
- I know that my use of the Internet is monitored and further action may be taken if a member of school staff is concerned about my safety
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- If I have permission to have my mobile phone at school, I will keep it switched off (not on silent mode) and hand it in to a member of staff before the start of the school day and collect it at the end of the day
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Name _____

Signed: _____

Class: _____

Date: _____

Bridgewater

Supporting Letter

Dear Parent / Carer

As part of an enriched curriculum your child will be accessing the Internet; viewing websites and using email.

In order to support the school in educating your child about Online safety (safe use of the Internet), please read and discuss the Online safety rules attached with your child then sign and return the slip below.

Should you have any concerns and wish to discuss the matter further please contact Mr Moralee via the school office.

Yours Sincerely

Mrs Robson
Headteacher

✂

Online safety Acceptable Use Rules Reply Slip

I have read and discussed the rules with _____ (child's name) and confirm that he/ she has understood what the rules mean and agrees to follow the Code of Conduct for Children to support the safe use of ICT at Bridgewater School.

Parent/ Carer Signature: _____

Print name: _____

Date: _____

Mobile Phone Policy

- Bridgewater School discourages Children from bringing mobile phones to school
- If a pupil needs to bring a mobile telephone to school for one day in an emergency, parents need to seek verbal permission from the Head or Deputy Head teacher
- The phone must be clearly labelled with the child's name, switched off and given in to a member of staff on arrival at school
- The phone must be collected at the end of the school day
- The phone must be concealed whilst leaving the school premises
- Where a pupil is found with a mobile in school, including the playground, the phone will be taken from the pupil and placed in the office. Parents will be contacted to collect the phone
- If a child is found taking photographs or video footage with a mobile phone of either Children or teachers, this will be regarded as a serious offence and the Head teacher will decide on appropriate disciplinary action. In certain circumstances, the pupil may be referred to the Police. If images of other children or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by an appropriate person
- Parents are advised that Bridgewater School accepts no liability for the loss or damage to mobile phones which are brought into the school
- If a child needs to contact his/her parents/guardians they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly

This policy became operational from March 2018 and
was reviewed Spring 2025
The policy may be amended from time to time in accordance with school development and any changes to legislation.

Mobile Device Policy

- Bridgewater School allows staff to bring in personal mobile phones and devices for their own use during non-contact rest periods only
- Under no circumstances does the Bridgewater School allow a member of staff to contact a pupil or parent/carer using their personal device
- Under no circumstances does the Bridgewater School allow a member of staff to photograph or video children on their personal device
- School devices will only be used to take photos or videos, when appropriate, where parental permission is in place
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Where the Bridgewater School/setting provides mobile devices for offsite visits and trips, only these devices should be used for any aspect of school business (e.g. contacting parents, taking photographs and videos, tweeting and Facebook status updates)
- Where the School/setting provides mobile devices for off-site school business, wherever possible these should not be taken home and should be stored in a secure location on school premises
- Staff should be mindful that photographs and video taken of colleagues during working hours should not be shared without permission of all those concerned and the Head teacher or equivalent
- Personal use of school owned devices is prohibited unless specifically approved by the Head teacher.
- Bridgewater School accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile devices
- It is the responsibility of parents and Children to ensure mobile devices are adequately insured
- If a pupil breaches these rules the device will be confiscated and given in to the main office. It will be returned to the pupil on receipt of a letter from parents. If another offence is committed then the phone will be confiscated and will only be returned to that pupil's parent/guardian in person

This policy became operational from March 2018 and reviewed Spring 2025.

The policy may be amended from time to time in accordance with school development and any changes to legislation.

Appendix V

Online safety Policy Checklist

An AUP should follow some general principles, summarised in the following ten points.

1. **Be clear and concise** Aim for an A4 page or two of core rules, issued as part of the home-school agreement or induction programme. You can supply more detail in a supplementary document.

2. **Be relevant to your setting** When creating your AUP, consider the needs and characteristics of your users, services and support networks. Bear in mind other policies – such as child protection, anti-bullying and behaviour policies. Ensure your AUP reflects these policies and vice versa.

3. **Encourage user input and ownership** Involve children and young people, parents and carers and people expected to enforce the AUP in developing and reviewing it. Users are more likely to keep to your AUP if they feel ownership of it.

4. **Write in an appropriate tone and style for users** Do you need different documents for younger and older Children, staff, parents and carers, or those with particular communication needs? If so, try and consult with each group and meet their needs (see example AUPs below).

5. **Promote positive uses of all technologies** Technology offers many wonderful opportunities. Promote the positives in your AUP rather than focusing on the negatives. Remember that technologies are evolving all the time. Reinforce the concept of safe and responsible use of all technologies in your AUP rather than referring to specific devices.

6. **Outline clearly acceptable and unacceptable behaviours** Users need to understand clearly what they can (and can't) do online using the technology and services available to them in the learning or care setting. They also need to understand how they can use their own equipment in certain settings. You may choose to ban all personal technology devices, or approve their use in certain situations, or encourage their use to support learning. Whatever you decide, make it clear.

7. **Outline clearly what network monitoring will take place** Users have a right to know how their network access will be monitored. An open and honest approach can help prevent challenges to authority should Online safety incidents occur.

8. **Outline clearly the sanctions for unacceptable use** Users need to understand what penalties they face if they break the rules. These may range from temporary suspension of services to disciplinary action or even legal intervention, depending on the seriousness of the incident.

9. **Review and update regularly** To remain effective, AUPs must be regularly reviewed and updated. In addition to a regular programme of review, AUPs should be reviewed more often if necessary. For example, as a response to emerging issues or serious Online safety incidents.

10. **Communicate regularly to all stakeholder groups** If you want users to keep to your AUP, they need to be aware of it and understand it. Consider the best approaches for introducing the AUP. Perhaps through the home–school agreement for Children and parents or carers, or within induction programmes for staff. Look for opportunities to assess whether the AUP is understood. Reinforce the AUP regularly, monitor its impact and ensure you communicate any changes.

Appendix VI

Online safety Policy Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the Online safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, Online safety Coordinator and Headteacher.

Does the school have an Online safety Policy?	Y/N
Date of latest update (at least annual):	
The policy was agreed by Governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator in school is:	
The Online safety Coordinator is:	
Has Online safety training been provided for all Children (age appropriate) and all members of staff?	Y/N
Is there a clear procedure for responding to an incident or concern?	Y/N
Do all staff sign a Code of Conduct or Acceptable Use Policy on appointment?	Y/N
Are all Children aware of the Online safety rules or Acceptable Use Policy?	Y/N
Are Online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all Children?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School Online safety rules?	Y/N
Are staff, Children, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	Y/N
Has the school-level filtering been designed to reflect educational objectives and been approved by the SLT?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of the SLT?	Y/N

Appendix VII
Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

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.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation, in England and Wales.

Sexual Offences Act 2003
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 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). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming 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 etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)
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 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.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files)
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.
The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
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.
Obscene Publications Act 1959 and 1964

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

Protection from Harassment 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.

This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person's life or injury to: anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic"

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Head Teachers have the power "to such an extent as is reasonable" to regulate the conduct of Children off site
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Appendix VIII
Further Information and Guidance

BBC
http://www.bbc.co.uk/cbbc/topics/stay-safe

CEOP (Child Exploitation and Online Protection Centre)
www.ceop.police.uk

Childline
www.childline.org.uk

Childnet
www.childnet.com

Digital Literacy
www.novemberlearning.com

Digizen.org.uk
http://www.digizen.org/

Information Commissioner's Office
www.ico.gov.uk

Internet Watch Foundation
www.iwf.org.uk

Kidsmart
www.kidsmart.org.uk

Newcastle Schools IT Support Team
Help with filtering and network security
Tel: (0191) 277 7282

South West Grid for Learning
http://www.swgfl.org.uk/OnlineSafety

Think U Know website
www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse
www.virtualglobaltaskforce.com

Acknowledgement
We gratefully acknowledge that this guidance is adapted from information provided by Kent, Hertfordshire County Council, South West and London Grid for Learning
Compiled by S. Khan, C. Johnston & J. Hughes