



E-Safety Policy 2020-21

Table of Contents

| | | |
|-------------------|---|----|
| 1.0 | Who will write and review the policy? | 3 |
| 2.0 | Teaching and Learning | 4 |
| 2.1 | Why is Internet use important? | 4 |
| 2.2 | How does Internet use benefit education? | 5 |
| 2.3 | How will pupils learn how to evaluate content? | 5 |
| | Managing Content and Communication | |
| 3.0 | How will email be managed? | 6 |
| 3.1 | Websites | 6 |
| 3.2 | Can pupil images and work be published? | 6 |
| 3.3 | How can emerging technologies be managed? | 6 |
| 3.4 | Mobile Phones | 7 |
| 3.5 | Laptops | |
| 3.6 | Prevent - Pupil log in | 7 |
| | Policy Decisions | |
| 4.0 | Internet access | 8 |
| 4.1 | Assessing risks | 8 |
| 4.2 | Handling e-Safety complaints | 8 |
| 4.3 | Cyberbullying | 9 |
| | Disseminating the Policy | |
| 5.0 | Sharing with pupils | 10 |
| 5.1 | Sharing with staff | 10 |
| 5.2 | Engaging parents | 10 |
| APPENDICES | | |
| I | Acceptable Use Agreement for Staff | 11 |
| II | Code of Conduct for Pupils | 12 |
| III | Supporting Letter (for parents) | 13 |
| IV | Laptop Policy | 14 |
| V | Mobile Phone Policy | 16 |
| VI | Photographs of Children - Parental Consent Form | 17 |
| VII | Video of Children - Parental Consent Form | 19 |
| VIII | e-Safety Policy Checklist | 20 |
| IX | e-Safety Policy Audit | 22 |
| X | Legal Requirements | 23 |
| XI | Further Supporting Materials | 26 |

1.0 Who will write and review the policy?

Review date: November 2020

| | |
|--|-----------------------|
| Senior Manager with responsibility for whole school Computing: | Allyson Thorpe |
| Computing Subject Leader: | J. Cowen |
| Safeguarding Responsibility: | Allyson Thorpe |
| ICT Governor: | Hudson Bell |

Monitoring of the Computing and e-Safety policy is the responsibility of the Computing Team and Senior Management of the school.

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

As e-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 e-Safety Coordinator in this school is Catherine Ramanandi 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 e-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), Childnet and Prevent.

Senior Management and Governors are updated by the Head Teacher and e-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 pupils, 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 Computing Policies

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 pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient

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

- Helping all children to engage in Computing with purpose and enjoyment
- Helping all children to develop the necessary computing skills
- Helping all children to become autonomous computational thinkers
- Helping all children to evaluate the benefits of Computing 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 Computing to develop partnerships beyond the school
- Celebrating success in the use of 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 along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet which may require access to online software. All pupils should be taught to use the Internet 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 How does Internet use benefit education?

Increased computer numbers and improved Internet access may be provided but its impact on pupils' learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and refine their publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

- The school's Internet access will be designed to enhance and extend education
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work
- Pupils will be given access to online programmes and software that will help develop their computational thinking

2.3 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content; for example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

The following statements require adaptation according to the pupils' age:

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of online materials is part of teaching/learning in every subject

3.0 How will email be managed?

- Pupils may only use approved email accounts
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone
- Whole-class or group email addresses will be used in primary schools for communication outside of the school
- Access in school to external, personal email accounts may/ will be blocked
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain messages is not permitted
- Staff should not use personal email accounts during school hours or for professional purposes

3.1 School website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. you could replace '@' with 'AT')
- The head teacher 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

3.2 Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused
- Pupils' 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 pupils are electronically published
- Pupil's work can only be published with their parent's permission, (see Appendix VI)

3.3 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.

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

3.4 Mobile Phones

Mobile phones are now a feature of modern society and most of our older pupils own one. The technology of mobile phones has developed such that they now have the facility to record sound, take photographs and video images. Therefore the school also recognises the advantages mobile phones have as a ubiquitous learning tool. However, this new technology is open to abuse leading to the invasion of privacy.

Increasing sophistication of mobile phone technology presents a number of issues for schools:

- They are valuable items that may be stolen
 - The integration of cameras into phones leading to potential child protection and data protection issues
 - The potential to use the phone e.g. for texting whilst on silent mode
 - Inappropriate messages being sent via SMS, including Cyberbullying, sexual harassment and grooming
 - Interruption to lessons and disrupting the learning of others
-
- Phones must always be switched off (not on silent mode) and handed in to the main office before the start of the school day, to be collected at the end of the day
 - If a pupil needs to contact his/her parents/guardians they will use a school phone in the main office
 - If parents need to contact children urgently they should always phone the school office
 - School accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile phones
 - It is the responsibility of parents and pupils to ensure mobile phones are adequately insured
 - If a pupil breaches these rules the phone 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

3.5 Laptops/Ipads

- Staff provided with a laptop/Ipad purchased by the school can only use it for private purposes at the discretion of the Headteacher. 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
- Staff provided with a laptop purchased by the school are responsible for updating the antivirus software
- Staff intending to bring personal laptops/Ipads on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop/Ipad
- Staff should not attach personal laptops to the school network
- The security of school laptops and Ipads are of prime importance due to their portable nature and them being susceptible to theft
- See School Laptop/Ipad policy (Appendix IV)

3.6 Prevent

- All children should use unique login details
- Children should not share login details with anyone
- Children should only use designated lpad that correspond to their name

4.0 Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's computers and Computing equipment
- All staff must read and sign the 'Acceptable use for staff agreement' before using any school Computing resources
- 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 pupils will be provided with supervised Internet access (see Appendix II)

4.1 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 Headteacher

4.2 Handling e-Safety complaints

- Complaints of Computing/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 Headteacher 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 Headteacher 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 Headteacher, 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, pupils and parents will be informed of the complaints procedure
- All staff, pupils and parents will be informed of the consequences of misusing the Internet and Computing equipment

4.3 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 will be clear procedures in place to support anyone affected by Cyberbullying
- All incidents of Cyberbullying reported to the school will be recorded

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

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence
- The school will take steps to identify the bully, where 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 bully 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 may be informed
- The police will be contacted if a criminal offence is suspected

5.0 Sharing with pupils

- e-Safety rules and posters will be displayed in all rooms where computers are used and highlighted/ discussed during Computing sessions
- Pupils will be made aware that the network and Internet use will be monitored
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use
- An e-Safety module will be included in the Computing scheme of work and Citizenship curriculum

5.1 Sharing with staff

- Staff will be consulted when creating and reviewing the e-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 Engaging parents

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website
- A parents' workshop will be held annually to inform parents/ carers about e-Safety issues and responsible use
- Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement (Appendix III)
- Information and guidance on e-Safety will be made available to parents/carers in a variety of formats (i.e. weblinks, printed documents, DVD, leaflets, presentations)

St John Vianney Primary School

Acceptable Use Agreement for Staff

Computing and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within school. To ensure that all adults within the school setting are aware of their responsibilities when using any form of Computing hardware and software all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provide positive role models to pupils for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the school equipment in an appropriate manner and for professional use in accordance with the e-Safety Policy
- I will not give out personal information (mobile phone number, personal e-mail address etc) to pupils or parents
- I will only use the approved, secure e-mail system (name.surname@stjohnvianney.newcastle.sch.uk) for any school business
- I know that I should complete virus checks on my laptop, memory stick and other portable devices so that I do not inadvertently transfer viruses onto the school network or other Computing equipment
- Only school purchased encrypted memory drives should be used by staff
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure school data is stored securely and used appropriately in accordance with school and other relevant policies
- I will report any accidental misuse of school Computing equipment, or accidental access to inappropriate material, to the Computing Subject Leader or Headteacher
- I will not connect any personal device (laptop, digital camera etc), to the school network without authorisation from the Headteacher
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Headteacher
- I will ensure that my online activity, both in and outside school, will not bring myself or the school into disrepute (this includes postings on social networking sites e.g. Facebook)

I have read, understood and agree to this code of conduct. I will support the safe and secure use of Computing throughout the school. I am aware I may face disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name: _____

St John Vianney Primary School

Code of Conduct for Pupils

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 using Computing equipment to communicate 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 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 only use the Ipad allocated to me
- I will inform a member of the teaching staff if I accidentally access inappropriate material
- I will inform a member of the teaching staff if I feel I or any of my peers have been contacted inappropriately
- I will not attempt to download any apps without the permission of the Computing subject leader
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- I will turn my phone off (not on silent mode) and hand it in to the main office 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

Signed: _____

Class: _____

Date: _____

St John Vianney Primary School

Laptop/Ipad/USB Policy for Staff

Staff provided with a **Laptop / Ipad / Encrypted USB** purchased by the school, agree to the following terms of use:

1. The **Laptop/Ipad/Encrypted USB** remains the property of St John Vianney Primary School and is for the use of the person it is issued to and must be returned to the school if and when the teacher leaves employment at the school.
2. The **Laptop/Ipad/ Encrypted USB** is open to scrutiny by senior management, contracted technicians and the ICT Subject Leader at school.
3. Insurance cover - via Newcastle City Council. It will be important to check with insurers that equipment to be taken off the premises is covered and you are satisfied on the level of any excess to be paid in the event of a claim. (Individual staff home contents insurance policies may apply- please note that most policies will not cover theft from cars).
4. Acceptable Use - teachers should accept and adhere to the school's Acceptable Use Policy, particularly with regard to Internet access.
5. The loading of additional software must be authorised by the school , support teaching and learning and be compliant with the following regulations:
 - **Copyright, Designs and Patents Act 1988**
Specifies that all software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.
 - **Computer Misuse Act 1990**
Identifies three main offences concerning unauthorised access to systems, software or data.

If you are in any doubt please speak to your school or LA before loading any software

6. Anti-Virus software must be installed and should be updated on a regular basis. School ICT staff will advise on the routines and schedule of this operation. Sophos anti-virus updates are available from school and are covered by the Local Authority licence.
7. Staff are responsible for updating and maintaining the antivirus software at home and/or bringing it into school to update.
8. All repair and maintenance of laptops/Ipads must be conducted under the terms and conditions of the warranty.

9. Data Protection - the terms of the school's Data Protection registration should be adhered to and users must clearly understand that there is a personal legal duty on them as well as the school.
10. Any charges incurred by users accessing the Internet from home are **not** chargeable to the school.
11. Staff should not connect personal laptops onto the school network.
12. Failure to comply with these guidelines and the school's Acceptable Use Policy, may result in the withdrawal of the equipment and may lead to disciplinary proceedings.
13. Storage Protection - It is the responsibility of the staff member to ensure the safety of all Laptops/Ipads/Encrypted USBs
14. **All confidential data must be stored in the Encrypted USB/Laptops/Ipads that are password protected. The use of non-encrypted USBs for school data is strictly forbidden.**

Laptop Details:

Make: _____

Model: _____

Serial Number: _____

Ipad Details:

Make: _____

Model: _____

Serial Number: _____

Authorised by Headteacher:

Signed: _____

Date: _____

Member of Staff:

Print name: _____

Signed: _____

Date: _____

St John Vianney Primary School

Mobile Phone Policy

- St John Vianney Primary School discourages pupils from bringing mobile phones to school
- If a pupil needs to bring a mobile telephone to school a request in writing needs to be made to the Headteacher
- 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 Headteacher
- The phone must be clearly labelled with the child's name, switched off and given in to the office on arrival at school
- The phone must be collected at the end of the school day from the office
- 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 pupil is found taking photographs or video footage with a mobile phone of either pupils or teachers, this will be regarded as a serious offence and the Headteacher will decide on appropriate disciplinary action. In certain circumstances, the pupil may be referred to the Police. If images of other pupils 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 St John Vianney Primary School accepts no liability for the loss or damage to mobile phones which are brought into the school
- If a pupil 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 15/11/2017
The policy may be amended from time to time in accordance with school development and any changes to legislation.

St John Vianney Primary School

Photographs of Children - Parental Consent Form

Name of Child: _____ Date of Birth: ___ / ___ / ___

St John Vianney Primary School would like to take photographs and or video recordings of pupils whilst they attend the school to celebrate their achievements and successes. Still or moving images may be published in our printed publications (e.g. School prospectus, newsletters), on our external website (www.stjohnvianney.newcastle.sch.uk). They may also be used to promote the good educational practice of the school to other teachers e.g. at training events organised by the Local Authority or national education/government institutions. Children's names will never be published alongside their photographs externally to the school. Names may be used internally, for example - on a display.

Photographs / videos may also be published for internal use only, as part of children's regular classroom work e.g. on classroom displays, within multimedia projects (e.g. PowerPoint), on the school's internal network and to share educational achievements with parents e.g. video presentation of a school trip. Electronic images, whether photographs or videos, will be stored securely on the school's network which is accessible only by authorised users. Before using any photographs/videos of your child we need your permission. Please answer questions 1 to 5 below, then sign and date the form where indicated.

Please return the completed form to the school office as soon as possible.

[Please delete]

1. May we use your child's photograph in printed publications produced by St John Vianney Primary School or Newcastle Local Authority?
Yes / No

2. May we use your child's photograph on our Internet website
 - a) as part of a large group or whole school activity?
Yes/No

 - b) showing an individual activity? (e.g. holding a winner's trophy)
Yes / No

3. May we allow your child's photograph (e.g. as part of a school team or record of a school event) to be used for publication in a newspaper?
Yes / No

4. May we use any photograph or video of your child internally as part of the regular curriculum and work of the school?
Yes / No

5. May we use any video containing your child to share good educational practice with teachers from other schools?
Yes / No

6. May we use photographs or video of your child for their class blog?

Yes / No

This form is valid from the date of signing until your child leaves the school. Photographs and videos may be securely archived after your child has left the school but will not be re-used or re-published externally without renewed consent. Archiving provides a valuable record of the school's history for future generations.

We recognise that parents, carers and family members will wish to record events such as school plays, sports days etc to celebrate their child's achievements. St John Vianney Primary School is happy to allow this on the understanding that such images/recordings are used for purely personal family use. A full copy of the school's policy on the safe use of children's photographs may be obtained upon request to the school office.

Signed: _____ Date: _____

Print name: _____

Appendix VIII

e-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 pupils, 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 e-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 e-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 pupils 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 IX

E-Safety Policy Audit

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

| | |
|---|-----------------|
| Does the school have an e-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 e-Safety Coordinator is: | |
| Has e-Safety training been provided for all pupils (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 pupils aware of the e-Safety rules or Acceptable Use Policy? | Y/N |
| Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? | Y/N |
| Do parents/carers sign and return an agreement that their child will comply with the School e-Safety rules? | Y/N |
| Are staff, pupils, 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 X

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 pupils 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 XI

Further Information and Guidance

Becta

www.becta.org.uk/safeguarding

BBC

www.bbc.co.uk/cbbc/help/safesurfing

CEOP (Child Exploitation and Online Protection Centre)

www.ceop.police.uk

Childline

www.childline.org.uk

Childnet

www.childnet.com

Click Clever Click Safe Campaign

<http://clickcleverclicksafe.direct.gov.uk>

Cybermentors

www.cybermentors.org.uk

Digital Literacy

www.novemberlearning.com

Digizen

www.digizen.org.uk

Information Commissioner's Office

www.ico.gov.uk

Internet Watch Foundation

www.iwf.org.uk

www.kenttrustweb.org.uk/kentict/kentict_home.cfm

Kidsmart

www.kidsmart.org.uk
www.netsmatzkids.org

Newcastle Schools IT Support Team

Help with filtering and network security

Tel: (0191) 277 7282

Teach Today

<http://en.teachtoday.eu>

Teachernet

www.teachernet.gov.uk

Think U Know website

www.thinkuknow.co.uk

Virtual Global Taskforce – Report Abuse

www.virtualglobaltaskforce.com

Prevent Strategy

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

Acknowledgement

We gratefully acknowledge that this guidance is adapted from information provided by **Kent Local Authority**