St Joseph's Catholic Primary School

Online Safety Policy 2019-2020

St. Joseph's Catholic Primary School

Mission Statement

At St. Joseph's we aim to

Promote a learning community

based on the Gospel values of love, trust and respect

where the achievements of everyone

are recognised and celebrated.

Living, Learning and Loving together with Christ.

Online Safety Policy

Statement

Online safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- Online safety is about safeguarding children and young people in the digital world.
- Online safety emphasises learning to understand and use new technologies in a positive way.
- Online safety is less about restriction and more about education regarding the risks as well as the benefits so we can feel confident online.
- Online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The School's Online Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

Autumn 2019
Due for review Autumn 2020

Table of Contents

APPENDICES

1.0 Who will write and review the policy?

Issue date: May 2018
Reviewed by: E Mathews
Ratified by Full Governors: 28 June, 2018
Review date: Autumn 2019

Senior Manager with responsibility for whole school computing: Miss E Mathews
Online Safety Co-ordinator/Computing Co-ordinator: Mrs L Noble
Computing Subject Lead: Mrs L Noble
Safeguarding Responsibility: Miss E Mathews
Technician: SLA with IT Assist
Computing Governor: Mr M Keller

Monitoring of the Online Safety Policy is the responsibility of the Computing Co-ordinator and the Leadership Team of the school.

The policy is reviewed each year by the Computing Co-ordinator and the 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 Computing Co-ordinator in this school is Mrs L Noble who has been designated this role as a member of the Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the Computing Co-ordinator 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 Leadership and Governors are updated by the Computing Co-ordinator 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 agreement for staff and Code of Conduct for 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 (including Anti-Bullying)
- PSHE
- Corporate ICT Policies

2. 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 pupils to use computing with purpose and enjoyment
- Helping all pupils to develop the necessary skills to exploit computing
- Helping all pupils to become autonomous users of computing
- Helping all pupils to evaluate the benefits of computing and its impact on society
- Meeting the requirements of the National Curriculum and helping all pupils 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. 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 Education – Pupils

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

- A planned Online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key Online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff 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 pupils 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.
- Where pupils are allowed to freely search the internet, staff are 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.

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, newsletters, websites, class dojo
- Parents' sessions
- High profile events / campaigns e.g. Safer Internet Day

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.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online safety provision.

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 is 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 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 Co-ordinator 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 Co-ordinator will provide advice / guidance / training to individuals as required.

2.6 Training – Governors

Governors will have the opportunity to take part in Online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

3. Use of mobile devices
3.1 Mobile Phones

Mobile phones are now a feature of modern society and most of our 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 an 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 and sexual harassment
- Interruption to lessons and disrupting the learning of others

Staff

- All staff mobile phones should be either switched off or on silent and put away in a cupboard/locker during the school day
- No member of staff should use a personal mobile phone in the presence of pupils
- Mobile phones may be used during break times but only in areas of the school where pupils are not present
- Staff should keep personal phone numbers private and not use their own mobile phones to contact pupils or parents
- Staff on school visits may take their mobile phones in case of emergency. **NB - they must only be used in the event of an emergency**. (All contact details for children/staff are kept on RM Integris, accessible on a school iPad. The iPad may also be used to take photographs/videos during the visit).
- Staff should keep a record of their phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure on school premises and report thefts immediately to the head teacher.

Pupils

- Pupils are not permitted to have mobile phones in school or on educational visits.
- If a pupil does bring a mobile phone into school, it must be switched off and handed in to the school office. It can be collected at the end of the school day.
- Children who do not abide by this rule will be disciplined in line with our Behaviour Policy.
- If parents need to contact their 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.

Visitors

- All visitors will be expected to refrain from using their mobile phone in school in the presence of pupils.

3.2 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
- Staff provided with a laptop purchased by the school are responsible for updating the antivirus software
- Personal laptops should not be used in school
- 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 (Appendix IV)

4. Use of digital media (cameras and recording devices)

4.1 Consent and Purpose

- Parents will give written consent at the beginning of each school year or on entry to school for photographs of their children to be taken or used. They may also be asked to give consent for certain activities children will be taking part in during the school year.
- Adults employed in school will give written consent at the beginning of each school year or on entry to school for photographs of themselves to be taken or used.
- It will be made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of third parties).
- Consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc. Images will be deleted when the child has reached the end of Year 6.
- Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press / other external media.
- A list of all children and adults who have requested that their photographs will not be taken or used is available in the school office.

4.2 Taking Photographs / Video

- All members of staff are authorised to take photographs/videos.
- All photographs/videos should be taken using school owned equipment. The use of personal equipment to store images is not allowed.
- When taking photographs/ video:
    - The rights of an individual to refuse to be photographed will be respected.
    - The photograph will not show children who are distressed, injured or in a context that could be embarrassing or misinterpreted.
    - Ensure that certain children are not continually favoured when taking images.
    - Ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted. This would include for example, considering the angle of shots for children engaged in PE activities.
    - Photographs of children or adults should not be taken in toilets or when changing for PE/Sport.

4.3 Parents Taking Photographs / Videos

Under the Data Protection Act (1998), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

- Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.
- Parents are asked to wait until the end of an event to take photographs / videos so as not to disrupt the event.
- Parents are reminded in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects.

4.4 Storage of Photographs / Video

- Photographs are securely stored on the school network
- Storage of photographs on USB memory sticks is not allowed.
- Storage of images on personal equipment e.g. tablets, laptops or USB storage devices is not allowed.
- Staff should not store personal images on school equipment.

- School staff have access to photographs / videos stored on school equipment.
- School staff are responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed.
- Should a parent withdraw permission for photographs / videos, a nominated member of staff will ensure that all images have been securely deleted.
- All images sent via email should be sent securely.

4.5 Publication of Photographs / Videos

When publishing images,

- Children's images should not be displayed on insecure sites e.g. personal Social Networking Sites.
- Full names and personal details will not be used on any digital media, particularly in association with photographs/ videos.

The Media, Third Parties and Copyright

- Third Parties are supervised at all times whilst in the school and permission is sought from parents prior to the taking of any photographs / videos.
- If uploading images to a third party website, e.g. for printing or creating calendars, cards etc, the terms and conditions of the web site must be read beforehand and agreed by the head teacher.

4.6 CCTV, Video Conferencing, VOIP and Webcams

- Parents are informed if CCTV, video conferencing or webcams are being used / in use in the school.
- Parents have given permission for their child/children to participate in activities that include taking of video and photographs.
- Video conferencing (or similar) sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- The purpose for video conferencing or webcams will be made clear to those liable to be included in footage taken by these resources.
- Notifications are in place to inform setting users that CCTV is being used.
- CCTV cameras are located throughout the school both indoors and outdoors. They do not overlook sensitive areas, e.g. changing rooms or toilets.
- Abel Alarm Company Limited manages the CCTV system. Recordings are stored on the hard drive on a 22 day cycle. Copies of recordings/images are made in the event of a request from police only.

5. Communication technologies

5.1 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 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

5.2 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

5.3 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 (parent's consent form)
- Pupils' work can only be published with their parent's permission (parent's consent form)

5.4 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.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The Computing Co-ordinator will carry out each risk assessment.

5.5 Social Networks

- If a social network site is used personally, staff must not share details with pupils and privacy settings should be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff must not give personal contact details to pupils or parents / carers.
- Staff should not befriend pupils or other members of the school community on social networking sites.
- Staff must not use school equipment to communicate with personal contacts (eg Facetime on an iPad).
- The content posted online <u>should not</u>:
    - Bring the school into disrepute
    - Lead to valid parental complaints
    - Be deemed as derogatory towards the school and / or its employees
    - Be deemed as derogatory towards pupils and / or parents and carers
    - Bring into question their appropriateness to work with children and young people

Inappropriate use of Social Networking sites – Action by the school:

Following a report of inappropriate use of social networking sites, the nominated person will take the following action.

- Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed.

- If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed.

- In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

- Before the nominated person contacts a service provider, he or she will check the location of the material – for example by taking a screen capture of the material that includes the URL or web address. If the nominated person is requesting that the service provider takes down material that is not illegal, he or she will be clear how it contravenes the site's terms and conditions.

Where the perpetrator is a member of the school community (including parents/carers) the school will:

- deal with harassment and bullying under the relevant school procedure;

- take care to make an informed evaluation of the severity of the incident;

- deliver appropriate and consistent sanctions; and

- provide full support to the staff member(s) affected.

The governing body recognises its legal duty to protect staff from unlawful harassment as well as mental and physical injury at work.

In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff and parents, where necessary.

6. Infrastructure and technology

6.1 Pupils' access

- Pupils are supervised by an adult when accessing school equipment and online materials
- Pupils have individual logins
- Pupils have restricted access to the school's network

6.2 Adult access

- Access to certain areas of the school's network are restricted to identified members of staff according to their areas of responsibility

6.3 Passwords

- All users of the school network have a secure username and password
- Staff and children are reminded of the importance of keeping passwords secure

6.4 Software/hardware

- The school has legal ownership of all software (including apps on tablet devices)
- There is an up to date record of appropriate licenses for all software and IT Assist (SLA) is responsible for maintaining this
- Equipment and software is audited on an annual basis
- The IT technician controls what software is installed on school systems

6.5 Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access is restricted
- Wireless devices are accessible only through a secure password
- The IT technician is responsible for managing the security of the school network and keeping the school systems up to date in terms of security
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password and permissions are assigned according to their role.
- Staff and pupils are required/reminded to lock or log out of a school system when a computer/digital device is left unattended
- The IT technician is responsible for assessing and installing new software
- Any suspicion or evidence of a breach of security should be reported to the head teacher.
- The IT technical support provider is aware of the school's requirements / standards regarding online safety
- Computing subject leader and the head teacher are responsible for liaising with the technical support staff

Filtering and virus protection

- Filtering is managed through the RM Education
- Staff are aware of the procedures for blocking and unblocking specific websites
- Staff are aware of the procedures for reporting suspected or actual computer virus infection. These should be reported to the head teacher immediately.

6.6 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

7. Dealing with incidents

7.1 Handling online safety complaints

- Complaints of computing/Internet misuse must be recorded and will be dealt with by the head teacher, 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, pupils and parent/carers will be informed of the complaint's procedure
- All staff, pupils and parents/carers will be informed of the consequences of misusing the Internet and computing equipment

7.2 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 should be reported to the head teacher at the earliest possible opportunity
- All incidents of cyberbullying reported to the school will be recorded
- Pupils, staff and parents/carers should keep a record of any incident as evidence

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

- 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
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases will be dealt with most effectively under the relevant school disciplinary procedure.
- Monitoring and confiscation must be proportionate to the incident. Except in exceptional circumstances (for example, where disclosure would prejudice the conduct of a criminal investigation) parents, employees and learners will be made aware, and their consent sought, in advance of any monitoring (for example, of e-mail or internet use) or the circumstances under which confiscation might take place.
- Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police inquiries.
- Where pupils are found to have made unfounded, malicious claims against staff members, relevant disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.
- Staff should report all incidents to the nominated person – head teacher. The nominated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

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

8. Disseminating the policy

8.1 Sharing with pupils

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

8.2 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

8.3 Engaging parents

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

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 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 Online Safety Policy
- I will only use school equipment to take photographs or videos in school or on educational visits
- I will not give out personal information (mobile phone number, personal e-mail address, social network sites etc) to pupils or parents
- I will only use the approved, secure e-mail system name@stjosephsrcprimary.co.uk for any school business
- I know that I should complete virus checks on my laptop and other portable devices so that I do not inadvertently transfer viruses onto the school network or other computing equipment
- 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, or accidental access to inappropriate material to the head teacher
- I will not connect any personal device (laptop, digital camera etc), to the school network without authorisation from the head teacher
- 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 head teacher
- 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: _____

Online Safety 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 computing 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
- I will not bring a mobile phone to school
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Child's name /
Signed: _____

Class: _____

Date: _____

St. Joseph's Catholic Primary School

Dear Parent / Carer

As part of an enriched curriculum your child will be accessing the Internet; viewing websites, posting blogs 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 Code of Conduct (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 the head teacher via the school office.

Best wishes

Headteacher

✂_____

Online Safety Code of Conduct Reply Slip

Please sign and return by Friday 21 September, 2018

I have read and discussed the Code of Conduct with

_____ (child's name)

and confirm that he/ she has understood what the rules mean and agrees to follow the online safety rules to support the safe use of computing at St. Joseph's Catholic Primary School

Parent/ Carer
Signature: _____

Print name: _____

Date: _____

St. Joseph's Catholic Primary School

Laptop Policy for Staff

Staff provided with a laptop purchased by the school, agree to the following terms of use:

1 The laptop remains the property of St. Joseph's Catholic 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 is open to scrutiny by senior management, contracted technicians and the Computing Subject Lead at school.

3 Insurance - The school insurance policy will cover laptops when teachers have them at home, as long as they are being used for school business. The policy will not cover any theft from an unattended vehicle when the laptop is being transported to and from school.

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 completed by IT Assist, 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.

6 Windows Enterprise Defender, Systems Centre Configuration Manager antivirus software must be installed and should be updated on a regular basis. IT Assist will advise on the routines and schedule of this operation.

7 Staff are responsible for updating and maintaining the antivirus software. This is actioned whenever staff log onto the internet. Staff must ensure they log on either at school or home on a regular and frequent basis.

8 All repair and maintenance of laptops 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 laptop and may lead to disciplinary proceedings.

Laptop Details:

Make: _____

Model: _____

Serial Number: _____

Authorised by Headteacher:

Signed: _____

Date: _____

Member of Staff:

Print name: _____

Signed: _____

Date: _____

Appendix V

St. Joseph's Catholic Primary School

iPad Policy for Staff

Staff provided with an iPad purchased by the school, agree to the following terms of use:

1. The iPad remains the property of St. Joseph's Catholic 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 iPad is open to scrutiny by senior management, contracted technicians and the Computing Subject Leader at school.

3. Insurance cover - The school insurance policy will cover iPad when teachers have them at home, as long as they are being used for school business. The policy will not cover any theft from an unattended vehicle when the iPad is being transported to and from school.

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 completed by IT Assist, 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.

6. IOS/Operating System software must be installed and should be updated on a regular basis. IT Assist will advise on the routines and schedule of this operation.

7. IOS/Operating System software is actioned on a regular and frequent basis by IT Assist, following the alert received from Apple.

8. All repair and maintenance of iPad 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 iPad 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 iPad and may lead to disciplinary proceedings.

iPad Details:

Make: _____

Model: _____

Serial Number: _____

Authorised by Headteacher:

Signed: _____

Date: _____

Member of Staff:

Print name: _____

Signed: _____

Date: _____

Appendix VI

Pupils' Mobile Phone Policy

- St. Joseph's Catholic Primary School does not allow pupils to bring 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 Headteacher
- The phone must be clearly labelled with the child's name, switched off and taken to the office on arrival at school
- The phone must be collected at the end of the school day from the office
- If a pupil is found with a mobile in school the phone will be taken from the pupil and placed in the office. Parents will be contacted to collect the phone
- Parents are advised that St. Joseph's Catholic Primary School accepts no liability for the loss or damage to mobile phones which are brought into the school
- 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
- If parents need to contact their children urgently they should phone the school office and a message will be relayed promptly

St. Joseph's Catholic Primary School

Staff Mobile Phone Policy

- All staff mobile phones should be either switched off or on silent and locked away securely during the school day
- No member of staff should use a personal mobile phone in the presence of pupils
- Mobile phones may be used during break times but only in the areas of school where pupils are not present
- Staff should keep personal phone numbers private and not use their own mobile phones to contact pupils or parents
- Staff should keep a record of their mobile phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure on school premises and report thefts immediately to the head teacher

St. Joseph's Catholic Primary School

Photographs of Children – Parental Consent Form

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

St. Joseph's Catholic 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) and/or on our external website www.stjosephsrcprimary.co.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. Joseph's Catholic 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

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. Joseph's Catholic Primary School is happy to allow this on the understanding that such images/recordings are used for purely personal family use.

Signed: _____ Date: _____

Print name: _____

St. Joseph's Catholic Primary School

Video of Children – Parental Consent Form

Your child has been selected for inclusion in a video which the following organisation wishes to take on the date(s) shown:

Organisation: _____

Date video to be taken: _____

The purpose(s) for which the video is to be taken:

_____

_____

This will be displayed in the following places (must clearly state "Internet address" if it is intended to publish via this medium):

_____

If you have any queries regarding use of the video or change your mind then please contact the above organisation at the following address:

_____

Declaration

Being the parent or person responsible, I grant permission for a video of my child to be used in printed and electronic (delete as appropriate) publicity materials generated by the organisation named above. I acknowledge that the video will only be used for the purpose(s) stated and that I have a right to change my mind.

Name of Child: _____

School year: _____

Your Name: _____

Signature: _____ Date ___ / ___ / ___

Appendix X

Online Safety 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 Safeguarding Lead, SENCO, Online Safety Co-ordinator and Head teacher.

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 Safeguarding Lead in school is:	
The Online Safety Co-ordinator is:	
Has online 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 online safety Code of Conduct?	**Y/N**
Are online 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's online 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 XI
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 XII
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