St Joseph's Catholic Primary School
Acceptable Use and Online Safety Policy

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Joseph's Catholic Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of St Joseph's Catholic Primary School
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Online Radicalisation (Radicalisation is the process by which an individual or group comes to adopt increasingly extreme political, social, or religious ideals and aspirations. The internet offers opportunities from online radicalisation to spread easily)

Scope

This policy applies to all members of the St Joseph's Catholic Primary School community (including staff, pupils, governors, parents / carers, volunteers and visitors) who have access to and are users of school Computer systems, both in and out of St Joseph's Catholic Primary School. The school is aware that all members of the school community are at risk of breaching Online Safety protocols.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

This policy is written by the ICT/ Online Safety Co-ordinator. It is shared with senior management and approved by the Governors. It is shared with the whole school community.

This policy works alongside a number of other policies in the school including:

- Behaviour Policy
- Child Protection and Safeguarding Policy
- PSHCE Policy
- Prevent Action Plan
- Computing Policy
- Data Security Policy
- Mobile Phone Policy

What is Online Safety?

Online Safety is defined as educating people about the benefits, risks and responsibilities of using the internet and electronic devices. Online Safety is:

- safeguarding children in the digital world
- not about restricting children, but educating them
- supporting children and young people to develop safer online behaviours both in and out of school.
- being educated ourselves to be able to support and help the children

Acceptable Use Agreement

All members of the school community are expected to follow the schools Acceptable Use Rules and agree to the Acceptable Use Agreement. There are differing agreements dependent on the member's role. The Acceptable Use Agreements include:

- Data and MLE Agreement (Appendix 1)
- Teacher Agreement (Appendix 2)
- Support Staff Agreement (Appendix 3)
- Mobile Device Agreement (Appendix 4)
- Governor Agreement (Appendix 5)
- Pupil/ Parent Agreement (Appendix 6)

Roles and Responsibilities

All staff have a duty of care to the pupils that are in our school. We are all responsible for all aspects of pupil safety, including online safety, whilst in school. We must teach the children Online Safety skills regularly to help them develop safe online behaviours. Any activity involving internet use needs to be carefully planned and assessed for risk to minimise the possibility of an Online Safety incident. If an Online Safety incident occurs outside of school and effects our children, the school must deal with the incident.

The following section outlines the Online Safety roles and responsibilities of individuals and groups within our school.

Governors:

The Governors are responsible for:

- The approval of the Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors receiving termly information about online safety incidents.
- Providing a member of the Governing Body to take on the role of monitoring online safety linked in with monitoring safeguarding and being a member of the Online Safety Group.
- Reading, understanding and signing the Governor Acceptable Use Policy (AUP).

Headteacher:

The Headteacher has a duty of care for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online safety is delegated to the Online Safety Co-ordinator. The head teacher is responsible for ensuring:

- That they, the Deputy Head and the Online Safety Co-ordinator are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- They receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Co-ordinator:

The Online Safety Co-ordinator has the day to day responsibility for online safety. The Online Safety Co-ordinator is responsible for:

- Leading the day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policy and documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Providing training and advice for all members of the school community
- Ensuring all pupils understand and follow the Online Safety and acceptable use policies
- Ensuring Online Safety is embedded into the curriculum
- Liaising with technical staff (beebug)
- Receiving Online Safety reports and logging Online Safety incidents
- Meeting with the Online Safety Group to discuss current issues and review incident logs
- Reporting regularly to the Headteacher with regards to Online Safety.

Technical Staff:

The ICT Co-ordinator and Technical Support (Beebug) are responsible for ensuring:

- That the schools technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets the required Online Safety technical requirements that may apply
- That users may only access the networks and devices through a properly enforced password protection policy.
- That the use of the network, internet, MLE, website, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Co-Ordinator and the Headteacher

Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and the current school Online Safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problems to the Online Safety Co-ordinator, Deputy Headteacher or Headteacher for investigation, action or sanction.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online Safety is embedded into their teaching and that sites are checked for suitability before using them with the pupils.

Safeguarding/ Child Protection Officer:

The safeguarding/ child protection officer should be trained in the Online Safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate online contact
- Potential or actual incidents of grooming
- Cyberbullying

Pupils:

The pupils are responsible for:

- Using the school system in accordance with the pupil acceptable use policy (AUP)
- Reporting an abuse, cyberbullying, misuse or access to inappropriate materials
- Understanding the importance of being safe online
- Adopting good Online Safety practice when using digital technologies outside of school and understanding that the school Online Safety policy covers their actions out of school, if related to school

Parents/ Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand the issues relating to Online Safety through parent workshops, Online Safety newsletters, website and MLE. Parents and Carers are encouraged to support the school in promoting good Online Safety practice, Parent Acceptable Use Policy (AUP) and follow the guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parent sections of the website and MLE
- Social Networking Sites
- Mobile Phones
- Their children's personal devices which access the internet.

School Computer System/ Data Security/Filtering/ Internet Access

Computer System Security:

- The Headteacher has overall responsibility for the security of the Computer systems.
- The school Computer systems are reviewed regularly.
- Virus protection (Sophos) is installed and updated regularly.
- Personal data sent over the Internet is encrypted.
- Use of portable storage media such as USB memory sticks, DVDs, CD-ROMs and other storage devices will be reviewed. Where applicable such devices will comply with latest guidance on Handling Sensitive Data. At the very least, all USB and portable drives used to store sensitive data are encrypted and password protected.
- See *Data Security Policy* for details about data security including physical security, system security and back up processes.

Password Security:

All users are provided with a username and password generated by LGFL Atomwide. The ICT Co-ordinator keeps an up to date record of users and their usernames. The "administrator" passwords for the school Computer system, used by Beebug, must also be available to the Headteacher and ICT Co-ordinator and kept in a secure place. All users with access to the Computer systems are responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping their password secure from other people.
- Staff and children should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- When leaving a computer for any length of time, everyone shall log off or lock the computer, using CTRL+ATL+DELETE.
- Passwords shall not be revealed to unauthorised persons.
- Passwords shall not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- All users must immediately report any suspicion or evidence that there has been a breach of security.
- All higher level users (eg Head, Deputy, Data Manager, ICT Co-ordinator) are required to change their passwords every 90 days to ensure security.

School's Information Systems (SIMs), MLE and Website Security:

- See Data Security Policy for information about physical and systems security of data held on the schools information systems.
- Staff are issued with individual usernames and passwords to access SIMs. Their access rights are related to their role.
- Data and MLE administrators will abide by and sign the Acceptable Use Policy (AUP) (Appendix 1)
- The point of contact on the website is the school address, school email and telephone number.
- Website photographs that include pupils are selected carefully and pupils' names are not used anywhere on the website or MLE when in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school web site (Appendix 7)
- The copyright of all material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Staff ensure that all materials used within the MLE will have been carefully selected for their teaching and learning value.
- Editorial control of subject or year group pages within the MLE is passed to teachers; they are expected to exercise this control with care and all due regard for their position of trust and duty of care.

Filtering:

- The school works in partnership with Parents, Beebug, the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school has different policy groups which entitles the users to different filtering access.
- If staff or pupils discover unsuitable sites, the URL and content is reported to the Internet Service Provider and Beebug by the Online Safety Co-ordinator. These URL's will be recorded on the Online Safety incident log.
- The school is provided with LGFL guidelines for filtering categories. The Online Safety Co-ordinator and Head Teacher then decide which categories are suitable for which user groups. The filtering strategy is selected to suit the age and curriculum requirements of the pupils. The filtering categories that are allowed and denied are available to be seen at the end of this policy. (Appendix 13)

Internet Access:

- The school keeps a record of all staff and pupils who are granted Internet access. The record is kept up-to-date, e.g. staff may leave or a pupil's access may be withdrawn.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents are informed that pupils will be provided with supervised Internet access.

Computer System Use:

- Adult users need to sign the Acceptable Use Policy. (Appendix 1-5)
- Parents/carers of children in Reception and KS1 are required to sign an acceptable use policy on behalf of their child. KS2 children sign the acceptable use policy themselves and their parents sign it too. (Appendix 6)
- In the Computer Suite, children under 7 years of age are accompanied by an adult when accessing the Internet. The Computer suite is available during lunch times for pupils in KS2 and is monitored by pupil ICT Leaders.
- Children without internet access have access to the mini-suite at breaks and lunch times which is monitored by pupil ICT Leaders. They also have the opportunity to attend a weekly ICT Club run by the ICT Leader.

Communication

A wide range of communication technologies are available and used within the school including email, teachers2parent's text system, parent pay, MLE and website. When using communicating technologies the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users are aware that their email communications are monitored. Therefore staff and pupils should only use the school email system to communicate with others.
- Users must immediately report any communication that makes them feel uncomfortable. If offensive, threatening or bullying in nature the user must not respond to any such communication.
- Any digital communication between staff and parents/pupils and the wider community must be made through official school communication systems and must be professional in tone and content.
- Pupils are taught about the Online Safety issues relating to communication and strategies to support the pupils if they come into contact with inappropriate communications.
- Personal information should not be posted on the school website or MLE and only official email address should be used to identify members of staff.

Mobile Phones/ Handheld Mobile Devices

Personal Mobiles – Staff

We recognise that mobile phones provide a useful means of communication. However staff should follow the rules with regards to using mobile phones at work:

- Staff are not permitted to make/receive calls/texts during contact time with children.
- Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer or handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones (inc. receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- It is also advised that staff security protect access to functions of their phone.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Head teacher / Deputy Head teacher aware of this and can have their phone in case of having to receive an emergency call.
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras and flip cameras.
- Staff should report any usage of mobile devices that causes them concern to the Head teacher/ Deputy Head teacher.

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication on off- site activities. However staff should ensure that:

- Mobile use on these occasions is appropriate and professional (and will never include taking photographs of children).

- Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the school office or via Teachers2Parents.

- Where parents are accompanying trips they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

Personal Mobiles – Pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- Pupils are not permitted to have mobile phones on their person at school or on trips

- If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school if they are traveling home on their own. The following procedure must be followed:

  - The parent and pupil must complete and sign the mobile phone permission form which can be obtained from the school office and must be returned to the school office before a mobile phone can be brought into school. The permission form must be signed by the parents, pupil and school. (See Appendix 1 for Mobile phone permission form)

  - Once the permission form has been completed the child can bring a mobile phone to school. The phone must be switched off and handed in to the school office first thing in the morning. This must be recorded in the Mobile Phone Record book. The phone can then be collected at home time. When the phone is collected the child must sign the Mobile Phone Records book to acknowledge that it has been collected. (The phone is left at the owner's own risk).

  - The phones will be kept in a locked container until the end of the school day

- Mobile phones brought to school without permission will be confiscated and parents will be asked to collect the phone at the end of the day.

Where mobile phones are used in or out of school to bully or intimidate others, then the head teacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site' .

Personal Mobiles- Volunteers, Visitors, Governors and Contractors

All Volunteers, Visitors, Governors and Contractors are expected to follow our mobile phone policy as it relates to staff whilst on the premises. On arrival, such visitors will be informed of our expectations around the use of mobile phones.

Personal Mobiles- Parents

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times.

We therefore ask that parents' usage of mobile phones, whilst on the school site is *courteous* and *appropriate* to the school environment.

We also allow parents to photograph or video school events such as shows or sports day using their mobile phones – **but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own**. Please refer to Guidance on the Use of Photographic Images and Videos of Children in Schools.

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. For more information and procedures please see the Mobile Phone Policy.

Social networking and personal publishing

The school is aware that social networking is used widely for professional and personal purposes. The school has a responsibility to provide guidance and training to ensure that all Social Networking use is safe and responsible.

Staff and Social Networking:

- Staff are trained, as a part of their Online Safety training, about the risks of social networking.
- Staff are advised not refer to matters of school business when engaging with or on social networking sites.
- Staff are advised to act professionally online

Pupils and Social Networking:

- Pupils do not have access to social networking sites on the school system.
- Pupils are advised of the age restrictions on social networking sites.
- Pupils are taught about the risks of social networking through their e-saefty lessons, e-saftey pages on MLE and focussed social networking workshops for year 5/6 pupils.
- Pupils are taught to follow the social networking rules. (Appendix 9)

Parents and Social Networking:

- Parents are advised to not post school matters on social networking sites.
- Parents have opportunities to find out more about social networking sites by attending parent workshop and access information through school Online Safety page on MLE
- Parents are advised to follow the school social media rules at home with their children. (Appendix 9)

Use of digital and video images

- Procedures and practice ensure website safety. A senior member of staff oversees and authorises the website's content and checks suitability.
- The school will not use the first name and last name of individuals in a photograph.
    - If the pupil is named, we will not use their photograph / video footage;
    - If the photograph / video is used, we will not name the pupil.
- We ensure that before any images are uploaded to our web site or published electronically they are re-named so that the name of the pupil cannot be read by right-clicking on the image.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school. (Appendix 7)
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year unless an item is specifically kept for a key school publication.
- At times when it is deemed appropriate, images will be saved on the public image folder for the children to access.
- Staff sign the school's Acceptable Use Policy (Appendix 1-5) and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- Pupils are only able to publish to their own 'safe' area on the MLE. Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work. Some children will be granted access to publish materials in public areas on the MLE such as the School Council Room and the Pupil Newsroom.
- Pupils are taught about how images can be abused in their Online Safety education programme.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

New Technologies

The digital age is ever changing and new technologies are consistently emerging. The school will ensure emerging technologies are examined for educational benefit and risks before use in school is allowed.

Training and Online Safety Education

Staff

All staff receives Online Safety training and understands their responsibilities. Training is offered as follows:

- A planned programme of formal Online Safety training is made available to staff.
- All new staff receives Online Safety training as part of their induction programme, ensuring that they fully understand the school Acceptable Use and Online Safety policy.
- The Online Safety/ICT Co-Ordinator receives regular updates through attendance at training sessions and by reviewing guidance documents released by CEOP / LGFL / LA and others.
- This Acceptable Use and Online Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety/ICT Co-Ordinator provides advice, guidance and training to individuals as required

Governors

Governors should take part in Online Safety training sessions, with particular importance for those who are involved in safeguarding and child protection. This is offered in a number of ways:

- Attendance at training provided by the Local Authority
- Participation in school training / information sessions for staff or parents

Pupils

The education of pupils in Online Safety is an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. The school uses a range of resources to help with teaching Online Safety include LGFL Online Safety and E-Literacy Framework, LGFL Online Safety programs e.g. me online, CEOP, Cyberpass, Think you Know and Hector the Protector.

Online Safety education is provided in the following ways:

- A planned Online Safety programme is provided as part of Computing / PSHCE / other lessons and is regularly revisited – this covers both the use of computers and new technologies in school and outside school. (Appendix 14)
- Key Online Safety messages are reinforced as part of a planned programme of assemblies.
- The school promotes and celebrates Safer Internet Day.
- Social Media Workshops are held for Year 5/6 pupils.
- Pupils are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information
- Pupils are helped to understand the need for the pupil AUP and Computing Rules (Appendix 8) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Children use the Online Safety hand to know what information they should not share online (Appendix 10)
- Children use the Social Media Rules when using social media outside of school. (Appendix 9)
- Pupils sign the school system and internet permission form.(Appendix 6)
- Rules for use of ICT Systems/internet are posted in all rooms (Appendix 8).
- Staff should act as good role models in their use of ICT, the internet and mobile devices

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school therefore seeks to provide information and awareness to parents and carers through:

- Online Safety Page on DB Primary
- Access to Online Safety policy
- Parents Training
- Parent leaflets
- Parent Acceptable Use and Permission Letter (see Appendix 6)

Reporting/ Complaints/ Sanctions

All staff and pupils have a responsibility to report Online Safety incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the pupils, staff or school.

Complaints:

- Responsibility for handling incidents is delegated to the Online Safety/ ICT Co-Ordinator, Deputy Head or Head teacher.
- The school has a responsibility to deal with cyber bullying reports whether it is happening inside school or outside school.
- Complaints about staff misuse will be referred to the Headteacher.
- Pupils and parents are informed of the complaints procedure.
- Parents and pupils should work in partnership with staff to resolve issues.
- The use of the CEOP button can be issued in serious Online Safety issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Online Safety incidents will be recorded on the Online Safety incident log by the Online Safety/ ICT Co-Ordinator, Deputy Head or Head teacher (Appendix 11.) The Incident Log shall be formally reviewed, and any outstanding actions delegated, by the Head teacher. The Log should be reviewed annually by the Governing Body.

Sanctions:

Pupils are expected to follow the Rules for responsible Internet and computer network use. (Appendix 8) If they are not followed then sanctions will follow. After discussion with class teacher, sanctions available include:

- Interview by Online Safety/ ICT Co-ordinator, Deputy Head or Headteacher
- Informing parents or carers;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system

(Appendix 12 - What if… guidance on handling different Online Safety issues)

Asset disposal

- Details of all school-owned hardware are recorded in a hardware inventory.
- Details of all school-owned software are recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. (Beebug) This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Policy

This policy has been written by the ICT Leader/Online Safety co-ordinator. The policy has then been shared with senior management and then shared with Governors. Governors are responsible for the approval of the Acceptable Use and Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports.

Policy Sharing- Pupils:

- Rules for Internet access are posted in all rooms where computers are used.
- Pupils are informed that Internet use will be monitored.
- Pupils sign the Pupil Acceptable Use Rules and are made aware of sanctions for misuse (Appendix 6)
- Instruction in responsible and safe use should precede Internet access.
- All Pupils are educated on Online Safety and digital literacy skills which include responsible Internet use will as part of the Computing and PSHCE programme covering both school and home use.

Policy Sharing- Staff and Governors

- All staff must accept the terms of the 'Acceptable Internet Use Agreement'. (Appendix 1-5)
- All staff including teachers, classroom assistants and support staff, are provided with the Acceptable use and Online Safety policy, and its importance explained.
- Staff are aware that Internet is monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the Acceptable use and Online Safety policy is provided as required.

Policy Sharing- Others

The Online Safety policy is made available on our school website.

REVIEW

The ICT Leader/Online Safety Co-ordinator and staff have reviewed this policy in March 2018.
The policy will be reviewed again in March 2020

Complied By: J Edwards March 2018	**Number:** 8
Ratified by Governors:	**Review Date:** March 2020

APPENDIX 1

Data and MLE Administrator confidentiality

When accessing data you must at all times comply with the Data Protection Act. Use of the data must be consistent with the purpose for which the system was constructed. Data must be processed securely and not be subject to any unauthorised use or disclosure.

Staff with responsibility for managing and accessing personal data in the school's Management Information System (e.g. Capita SIMS) or the MLE (DB Primary), or any other systems linked to them, are strongly advised to agree to and comply with the following conditions:

1. The data is to be used only for educational purposes and in the interests of the person to whom that data belongs, and not for any other purposes.

2. Personal data is to be shared only with those who need the information to discharge a statutory education function.

3. Only authorised users may access the system and they must never share their login details with anyone.

4. Management of DB Primary usernames and passwords is the responsibility of the authorised system manager / DB Primary administrator in the school. Where necessary this responsibility may be shared with the authorised system manager in the LA and the system supplier.

5. Care must be taken to protect any data which is printed or otherwise displayed.

6. Procedures should be in place to protect any data in transit. Data must never be taken out of the system in an unencrypted form.

7. Temporary data sets must be deleted as soon as possible.

Name: _____

Signature: _____

Date: _____

APPENDIX 2

Teachers Agreement

The computer network, school laptops and mobile devices are owned by the school and are made available to staff to enhance their professional activities including teaching, research, administration and management.

- It is essential that staff realise that use of the school network, computers and laptops will be monitored and they will be held accountable for any misuse.

- The school reserves the right to examine or delete any files that may be held on its computer network or portable computers.

- Access should only be made via the authorised personal username and password, which should not be made available to any other person.

- Staff should not attempt to bypass the school Internet filtering system.

- Irresponsible use may result in the loss of Internet access and use of school owned laptop.

- If a school laptop is taken home staff should ensure that other family members do not use it.

- School laptops regularly used at home should be brought into the school from time to time to enable the laptop anti-virus and anti-spyware software to be updated.

- Any data concerning pupils should not be taken from the school and stored on a laptop, hard drive or pen drive unless the drive has appropriate data encryption enabled. (Please use the school encrypted USB pen provided)

- Staff are responsible for all email sent and for contacts made that may result in email being received. As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied for letters and other media.

- Posting anonymous messages and forwarding chain letters is forbidden.

- Copyright of materials must be respected and sources acknowledged when used.

- Use of school equipment to access inappropriate materials such as pornographic, racist or offensive material is forbidden. Use for personal financial gain, gambling, political purposes or advertising is forbidden. Social networking sites should not be accessed using school equipment.

- Video sharing websites such as YouTube should be used with extreme caution.

- Mobile phones (or similar mobile devices that can access the Internet, record and transmit text, sound, images, etc.) will not be used during lessons or whilst pupils are present unless in the case of emergency. Mobile phones / personal equipment should not be used for taking pictures of pupils.

- All use of school ICT equipment will be in compliance with the school's Acceptable Use of ICT Systems policy, which I have read.

- When using ICT equipment it is your responsibility to sign it out and in when using it.

- Think carefully before printing and ensure that it is collected from the printer. Only print in colour if it is absolutely necessary.

- **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.

- Staff must log onto DB Primary and check their lgfl staffmail accounts daily.

- Staff must follow DB Primary Expectations for updating DB pages

Name: _____

Signature: _____

Date: _____

APPENDIX 3

Support Staff Agreement

The computer network is made available to staff to enhance their professional activities including teaching, research, administration and management.

- It is essential that staff realise that use of the school network, computers and laptops will be monitored and they will be held accountable for any misuse.
- The school reserves the right to examine or delete any files that may be held on its computer network or portable computers.
- Access should only be made via the authorised personal username and password, which should not be made available to any other person.
- Staff should not attempt to bypass the school Internet filtering system.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials must be respected and sources acknowledged when used.
- Use of school equipment to access inappropriate materials such as pornographic, racist or offensive material is forbidden. Use for personal financial gain, gambling, political purposes or advertising is forbidden. Social networking sites should not be accessed using school equipment.
- Video sharing websites such as YouTube should be used with extreme caution.
- Mobile phones (or similar mobile devices that can access the Internet, record and transmit text, sound, images, etc.) will not be used during lessons or whilst pupils are present unless in the case of emergency. Mobile phones / personal equipment should not be used for taking pictures of pupils.
- All use of school ICT equipment will be in compliance with the school's Acceptable Use of ICT Systems policy, which I have read.
- When using ICT equipment it is your responsibility to sign it out and in when using it.

- Think carefully before printing and ensure that it is collected from the printer. Only print in colour if it is absolutely necessary.

- **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.

- Staff must log onto DB Primary and check their lgfl staffmail accounts daily.

Name: _____

Signature: _____

Date: _____

APPENDIX 4

Governors Agreement

The school MLE (DB Primary) and email is made available to Governors for administration and management of governor duties.

- It is essential that Governors realise that use of the DB Primary will be monitored and they will be held accountable for any misuse.
- Only authorised users may access the system and they must never share their login details with anyone.
- Emails relating to governor duties should be sent and received via your LGFL account.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Confidential information is to be shared only with those who need the information to discharge a statutory governor function.
- Care must be taken to protect any confidential governor information which is printed or otherwise displayed.
- Do not leave sensitive or confidential data on printers, computer monitors or desk whilst away from your desk or computer.
- Copyright of materials must be respected and sources acknowledged when used.
- Governors must log onto DB Primary and check their lgfl staffmail accounts weekly.

Name: _____

Signature: _____

Date: _____

APPENDIX 5

Mobile Device Teachers Agreement

The mobile devices are owned by the school and are available for staff to enhance their professional activities including teaching, assessment, and administration.

- The Teacher mobile devices are for the use of teachers only and should not be used by the children.

- The use of the school network and mobile device will be monitored and teachers will be held accountable for any misuse.

- The school reserves the right to examine or delete any apps or files that may be held on the mobile device.

- Use of the mobile device to access inappropriate materials such as pornographic, racist or offensive material is forbidden. Use for personal financial gain, gambling, political purposes or advertising is forbidden. Social networking sites should not be accessed using the mobile device.

- Irresponsible use may result in the loss of the mobile device.

- The mobile device may be taken off site, however if the mobile device is lost, stolen or damaged off site it will be the teachers responsibility to replace the device.

- If the mobile device is taken home teachers should ensure that other family members do not use it.

Name: _____

Signature: _____

Date: _____

APPENDIX 6

Pupil and Parent AUP- Parental Permission

Dear Parents,

Acceptable use of the Internet, Computer Network and Other Computing Equipment

The use of ICT (Information and Communication Technology) including the Internet, email, school computing network, online learning tools (DB Priamry, Bug Club, My Maths, Purple Mash), and computing equipment are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

The school has updated the Pupil Acceptable Use Rules and Parent Acceptable Use Agreement to ensure all users are kept safe when using the computing network, internet and other computing equipment. These rules outline how we expect our pupils to behave to ensure they act in a responsible and safe way when using technology. The Parent Agreement outlines how Parents use the internet, digital images and social networking in a safe and responsible way to ensure we protect our children from any Online Safety risks.

Please share and discuss the attached Pupil Acceptable Use Rules with your child. After you have shared these rules we ask that all children and parents sign the Pupil Acceptable Use Rules.

After this has been signed, we ask Parents to read the Parents Acceptable Use Agreement, which is on the reverse of the Pupil Acceptable Use Rules, and to sign this before returning the form to school.

Please note if you have more than one child in the school you will need to complete the form for each child.

Signing the School Acceptable Use Rules/ Agreement helps us to maintain responsible use of ICT and safeguards the pupils in school.

If you have any concerns or would like to discuss any aspect of the use of ICT in school, do not hesitate to get in contact.

Please can the Acceptable Use forms be returned to school by …..

Yours sincerely,

Miss J Edwards
ICT Leader

Pupil Acceptable Use Rules

Pupil Name: _____

Please read the Acceptable Use Rules and sign to say you agree to the rules.

- I will only use the computers for school work, educational games and homework.
- I will only use the school computer network with my own username and password which I will keep private.
- I will look after all ICT equipment I use at school.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring in storage devices from outside school unless I have asked my teacher.
- I will ask permission from my teacher before using the internet.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- If I am communicating online I will always be polite and sensible.
- I will not share any personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet.
- I will use Hector to protect my screen if I find anything I don't like and I will tell an adult.
- I will report any unpleasant material or messages. I understand my report would help protect others and myself.
- I understand that the school may check my computer files and look at the internet sites I have visited.
- I understand that any misuse of the schools computing network or internet may result in my access being taken away and my parents will be informed.

Pupil Agreement

I have read and understand these rules and agree to them.

Signed: _____ (Pupil)

Parent Agreement

As the parent or legal guardian of the pupil signing above, I grant permission for my child to use the school computing system, internet and other computing equipment.

Signed: _____ (Parent)

Parent Acceptable Use Agreement

Internet and ICT

- As the parent or legal guardian of the pupil named on the reverse, I grant permission for the school to give my child access to:
    - the computing network
    - the Internet
    - the online learning tools (DB Primary, Bug Club, Mathletics, Purple Mash)
    - computing equipment
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
- I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's Online Safety or e-behaviour they will contact me.

Use of digital images, photography and video

- I understand I am allowed to take photos and videos of my child at school events but I will not publish them online (e.g social networks) without permission from all of the people that are in the photo or video. I understand that this is to protect and safeguard all children.

Social networking and media sites

- I understand that the use of Social Networking to discuss school matters should not include any inappropriate comments to do with staff, pupils, other parents, concerns or complaints. If I have any concerns or complaints I will contact the school directly.

Mobile Phones

- I understand that I should use my mobile phone in a courteous and appropriate manner when on the school site.
- I understand that if I am accompanying the school on a school trip or sporting event I will not make contact with other parents (via calls, text, email or social networking) during the trip or use my mobile phone to take photographs of the children.

Summary

- I understand that the school takes any inappropriate behaviour seriously and will respond to any inappropriate or unsafe behaviour that occurs within school or outside of school.
- I understand I can report Online Safety matters to the school and they will help or advise me on how to deal with the issue.
- I will support the school by promoting safe use of the Internet, digital technology and social networks at home. I will inform the school if I have any concerns.

Parent Agreement

I have read the Acceptable Use Agreement above and agree to support the school.

Signed: _____ (Parent)

APPENDIX 7

ST JOSEPH'S CATHOLIC PRIMARY SCHOOL
CONSENT FORM

CHILD'S SURNAME …… … CLASS ……..

CHILD'S FIRST NAME …… DATE OF BIRTH ……..

PRINT NAME OF SIGNATORY …….

1. Photographs in the Media

I have no objection to my son's / daughter's photographic appearance in the Media and on the School Website.

Signed ……. Parent / Carer Date ……...

2. School Outing

I give permission for my child to be taken on any organised local educational school visit arranged by the school.

Signed …… Parent / Carer Date ……...

3. Medical Emergency

In case of a medical emergency, I give permission for my child to be taken to hospital by ambulance accompanied by a member of the school staff. If I cannot be contacted, I give permission for the member of school staff to act on my behalf and authorize any emergency medical treatment advised by the hospital staff.

Signed …….. Parent / Carer Date ……

4. Home / School Agreement

I have read and discussed with my child the contents of the Home / School Agreement and agree to support the school in its implementation.

Signed …… Parent / Carer Date ……...

5. Internet Permission Form

I have read the rules and give permission for my child to use electronic mail and the Internet. I understand that pupils will be held responsible for their own actions.

Signed …….. Parent / Carer Date ……...

6. Library Consent

I have read the letter regarding the school library. I agree to the terms and conditions of my child using the St Joseph's School Library.

Signed …….. Parent / Carer Date …….

APPENDIX 8

Pupil Rules for responsible Internet and computer network use

These rules will help us to be safe and responsible users.
They will help to keep everyone safe.

- I will keep the ICT suite tidy when I use it.
- I will look after all ICT equipment.
- I will not bring food or drinks into the ICT suite.
- I will only use the system with my own username and password which I will keep secret.
- I will only use the computers for school work, DB Primary work, educational games and homework.
- I will only print with my teachers or ICT leaders permission.
- I will ask permission from my teacher or ICT leaders before using the internet.
- I will not bring in storage devices from outside school unless I have asked my teacher.
- I will use Hector to protect my screen if I find anything I don't like and I will tell my teacher.
- I will not give my home address or telephone number or arrange to meet anyone over the internet.
- The messages I add to DB Priamry forums will be polite and responsible.
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect others and myself.
- I understand that the school may check my computer files and look at the internet sites I have visited.

After discussion with class teacher, sanctions available include:

- interview with ICT Leader or Headteacher
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system

APPENDIX 9

Social Networking Rules

- Don’t give out your personal information
- Don’t use your personal information to create your username or screenname
- Only be friends with people you know in real life
- Never meet someone you met online
- Think carefully before you post online because once it is posted its difficult to remove
- Never post anything that could upset someone
- Only post things you would be happy for your Teacher or Parent to see
- Tell an adult if you see upsetting language, nasty picture or if you are being cyberbullied
- Tell an adult If you know someone is getting cyberbullied or you know someone isn't using the internet properly
- Think about your online reputation and digital footprint
- Be responsible for your own actions

APPENDIX 10
Online Safety Hand

APPENDIX 11

St Josephs **Online Safety Incident Log**

Details of ALL eSafety incidents to be recorded by the Headteacher or Deputy Head. This incident log will be monitored termly by the Headteacher and Chair of Governors

Date & Time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

APPENDIX 12

ONLINE SAFETY INCIDENT GUIDANCE: What if…

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

- Play the situation down; don't make it into a drama.
- Report to the ICT Leader/Deputy Headteacher/ Headteacher and decide whether to inform parents of any Pupils who viewed the site.
- Inform Beebug/LGFL and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
- Enter on the Online Safety Incident Log

An inappropriate website is accessed <u>intentionally</u> by a child.

- Refer to the Acceptable Use Form that was signed by the child, and apply agreed sanctions.
- Notify the parents of the child.
- Inform Beebug/LGFL and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
- Enter on the Online Safety Incident Log

An adult uses School ICT equipment inappropriately.

- Ensure you have a colleague with you, do not view the misuse alone.
- Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
- Enter on the Online Safety Incident Log
- If the material is offensive but not illegal, the head teacher should then:
  - Remove the PC to a secure place.
  - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
  - Identify the precise details of the material.
  - Take appropriate disciplinary action (contact Personnel/Human Resources).
  - Inform governors of the incident.
- In an extreme case where the material is of an illegal nature:
  - Contact the local police or High Tech Crime Unit and follow their advice.
  - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email, messaging or mobile phone technology, either inside or outside of school time.

- Advise the child not to respond to the message and save any messages received.
- Refer to relevant policies including Online Safety anti-bullying and PSHCE and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's e-mail service provider.
- Notify parents of the Pupils involved.
- Consider delivering a parent workshop for the school community.
- Inform the police if necessary.
- Enter on the Online Safety Incident Log

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
- Endeavour to trace the origin and inform police as appropriate.
- The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

- Report to and discuss with the named child protection officer in school and contact parents.
- Advise the child on how to terminate the communication and save all evidence.
- Contact CEOP http://www.ceop.gov.uk/
- Consider the involvement police and social services.
- Enter on the Online Safety Incident Log
- Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the ICT Leader, Deputy Head or Headteacher.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

APPENDIX 13

Filtering Categories for St Joseph's Catholic Primary School in Harrow (310-3507)

Category	Set By	Linux Proxy	Staff	Students
Abortion - Prochoice	Local	Allowed	Denied	Denied
Abortion - Prolife	Local	Allowed	Denied	Denied
Abortions	Local	Denied	Denied	Denied
Activist/Advocacy Groups	Local	Allowed	Allowed	Denied
Adult Content	Local	Allowed	Denied	Denied
Adult Image	Local	Allowed	Denied	Denied
Advertising	Local	Allowed	Allowed	Allowed
Adware	Local	Allowed	Allowed	Allowed
Alcohol	Local	Allowed	Allowed	Allowed
Alternative Lifestyles	Local	Allowed	Allowed	Denied
Arts & Culture	Local	Allowed	Allowed	Allowed
Bad Link	Local	Allowed	Denied	Denied
Banner/Ad Servers	Local	Allowed	Allowed	Denied
Blogging	Local	Allowed	Allowed	Allowed
Bullying	Local	Allowed	Allowed	Denied
Classifieds	Local	Allowed	Allowed	Allowed
Computer Security	Local	Allowed	Allowed	Allowed
Criminal Skills	Local	Allowed	Denied	Denied
Culinary	Local	Allowed	Allowed	Allowed
Directory	Local	Allowed	Allowed	Allowed
Drugs - Debate	Local	Allowed	Allowed	Denied
Drugs - Illegal	Local	Allowed	Allowed	Denied
Drugs - Prescribed	Local	Allowed	Allowed	Allowed
Education	Local	Allowed	Allowed	Allowed
Educational Games	Local	Allowed	Allowed	Allowed
Email	Local	Allowed	Allowed	Allowed
Entertainment	Local	Allowed	Allowed	Denied
Environmental	Local	Allowed	Allowed	Allowed
Extreme	Local	Allowed	Denied	Denied
File Sharing	Local	Allowed	Allowed	Denied
Forums	Local	Allowed	Allowed	Allowed
Freeware Downloads	Local	Allowed	Denied	Denied
Gambling	Local	Allowed	Denied	Denied
Games	Local	Allowed	Allowed	Allowed
Gay & Lesbian Issues	Local	Allowed	Denied	Denied
General	Local	Allowed	Allowed	Allowed
General News	Local	Allowed	Allowed	Allowed
Hate Speech	Local	Allowed	Denied	Denied
Host is an IP	Local	Allowed	Allowed	Allowed
Humor	Local	Allowed	Allowed	Allowed
Images	Local	Allowed	Allowed	Allowed
Infected Hosts	RBC	Denied	Denied	Denied
Instant Messaging (IM)	Local	Allowed	Denied	Denied
Internet Auction	Local	Allowed	Allowed	Denied

Intimate Apparel	Local	**Denied**	**Denied**	**Denied**
Intranet Servers	Local	**Allowed**	**Allowed**	**Allowed**
Investing	Local	**Allowed**	**Allowed**	**Denied**
Job Search	Local	**Allowed**	**Allowed**	**Allowed**
Journals and Blogs	Local	**Allowed**	**Allowed**	**Allowed**
Legal	Local	**Allowed**	**Allowed**	**Denied**
Malformed URL	Local	**Allowed**	**Denied**	**Denied**
Match Making	Local	**Allowed**	**Denied**	**Denied**
Matrimonial	Local	**Allowed**	**Allowed**	**Allowed**
Media Protocols	Local	**Allowed**	**Allowed**	**Allowed**
Medical	Local	**Allowed**	**Allowed**	**Denied**
Medication	Local	**Allowed**	**Allowed**	**Denied**
Misc Protocols	Local	**Allowed**	**Allowed**	**Allowed**
Music Downloads	Local	**Allowed**	**Allowed**	**Denied**
Network Unavailable	Local	**Allowed**	**Denied**	**Denied**
New URL	Local	**Allowed**	**Allowed**	**Denied**
No Text	Local	**Allowed**	**Allowed**	**Denied**
Nudity	Local	**Denied**	**Denied**	**Denied**
Occult	Local	**Allowed**	**Denied**	**Denied**
Online Sales	Local	**Allowed**	**Allowed**	**Denied**
Open Resource Sharing	Local	**Allowed**	**Allowed**	**Denied**
Parked	Local	**Denied**	**Denied**	**Denied**
Pay to Surf	Local	**Allowed**	**Denied**	**Denied**
Peer to Peer	Local	**Allowed**	**Denied**	**Denied**
Phishing	RBC	**Denied**	**Denied**	**Denied**
Phone Cards	Local	**Allowed**	**Denied**	**Denied**
Political	Local	**Allowed**	**Allowed**	**Allowed**
Portals	Local	**Allowed**	**Allowed**	**Denied**
Profanity	Local	**Allowed**	**Denied**	**Denied**
Proxy Anonymizer	RBC	**Denied**	**Denied**	**Denied**
Real Estate	Local	**Allowed**	**Allowed**	**Denied**
Redirector Page	Local	**Allowed**	**Allowed**	**Allowed**
Religion	Local	**Allowed**	**Allowed**	**Allowed**
Ringtones	Local	**Allowed**	**Denied**	**Denied**
Safe Search	Local	**Allowed**	**Allowed**	**Allowed**
Sales	Local	**Allowed**	**Allowed**	**Denied**
Search Engine	Local	**Allowed**	**Allowed**	**Allowed**
Search Keywords	Local	**Allowed**	**Allowed**	**Allowed**
Security Threat	RBC	**Denied**	**Denied**	**Denied**
Self Help	Local	**Allowed**	**Allowed**	**Allowed**
Sex Education	Local	**Allowed**	**Allowed**	**Denied**
SMS Messaging	Local	**Allowed**	**Allowed**	**Denied**
Social Issues and Support	Local	**Allowed**	**Allowed**	**Allowed**
Social Networking	Local	**Allowed**	**Allowed**	**Denied**
Sport - Hunting and Gun Clubs	Local	**Allowed**	**Denied**	**Denied**
Sports	Local	**Allowed**	**Allowed**	**Allowed**
Streaming Media	Local	**Allowed**	**Allowed**	**Allowed**
Substance Abuse	Local	**Allowed**	**Denied**	**Denied**

Tasteless/Illegal/Questionable	Local	**Allowed**	**Denied**	**Denied**
Technology	Local	**Allowed**	**Allowed**	**Allowed**
Tobacco	Local	**Denied**	**Denied**	**Denied**
Travel	Local	**Allowed**	**Allowed**	**Allowed**
Under Construction	Local	**Allowed**	**Allowed**	**Allowed**
URL Translation	Local	**Allowed**	**Allowed**	**Allowed**
Violence	Local	**Allowed**	**Denied**	**Denied**
Viruses	RBC	**Denied**	**Denied**	**Denied**
Voice Over IP (VOIP)	Local	**Allowed**	**Allowed**	**Denied**
Weapons	Local	**Allowed**	**Denied**	**Denied**
Web Chat	Local	**Allowed**	**Allowed**	**Denied**
Web E-mail	Local	**Allowed**	**Allowed**	**Denied**
Web Hosting	Local	**Allowed**	**Allowed**	**Denied**
Web Storage	Local	**Allowed**	**Allowed**	**Allowed**
Web-Based Chat & Email	Local	**Allowed**	**Allowed**	**Denied**

APPENDIX 14

St Joseph's Online Safety Scheme of Work

The delivery of a robust Online Safety curriculum is essential in ensuring our pupils are fully prepared for today's technological challenges.
This scheme draws upon E- Safety guidance that has been produced for schools from Becta (Signposts to Safety Teaching Online Safety at Key Stages 1 and 2)

Many of the resources used are available from the internet, however, those from CEOP ThinkUknow (Hectors World, Lee & Kim) have been downloaded onto the School Computer System.
There are 3 distinct areas to be covered:

1. E-Awareness – becoming aware of the online world
2. Online Research – developing the skills needed for safe online usage
3. Communication and Collaboration – develop an awareness of on-line communication

All classes should be taught one area per term:

- E-Awareness- Autumn Term
- Online Research – Spring term
- Communication and Collaboration – Summer Term

In addition Teachers should refer to all aspects of Online Safety that are in the Rising Stars Switched on Computing Scheme of Work Topics.

When planning your Online Safety lessons, please use the planning template provided and save in the Online Safety folder.

All resources, blank planning template and the scheme of work are saved on the system in the following location:

- Teach Only
- Online Safety
- Year Group Files

Additional resources: Year 1/2: LGFL Me Online Year 3/4:LGFL Our Online World Year 5/6: LGFL CyberPass

Online Safety			EYFS
PoS Statement (EYFS expectation)	• Select and use technology [safely] for particular purposes.		
	Learning Objectives:	**Teaching Points:**	**Possible Resources:**
Online Exploration	Children are aware that they can use the internet to play and learn, supported by a trusted adult/teacher. Children begin to understand the difference between real and online experiences.	Children need help from their teacher or trusted adult before they go online. Children explore onscreen activities that mimic real life. Children talk about the differences between real and online experiences.	**Online Resources** Poisson Rouge ICT Games Cbeebies games Fun with Spot http://www.bbc.co.uk/learningzone/clips www.kenttrustweb.org.uk
Online Communication & E-Awareness	Children know that they can use the Internet to communicate with family and friends. For children to understand the importance of politeness and courtesy on and off the internet. Children will be aware of how to keep safe and what to do if they are concerned.	Children begin to understand that they can share information online, e.g. via email or the school learning platform. Children begin to understand that there is a right and wrong way to communicate and this may be different depending on who you are communicating with.	**Online Resources** Sebastian Swan – visit Sebastian's blog and contact Sebastian Swan Smartie The Penguin story from KidSMART Time to Chat to accompany the Smartie e-book. **Think You Know Lee and Kim's Adventure** Activities 1B & 2B - Animal Magic Activity 6B – Song and Dance Activity 8 – Dot-to-dot Activity 9 – Making Masks or Puppets

Online Safety	Year 1
National Curriculum PoS Statement	• Use technology safely and respectfully, keeping personal information private. • Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Children begin to identify characteristics of people who are worthy of their trust. Children know what is meant by personal information and develop awareness of why it is special.	Know that some information (full name, address, birthday etc…) is special as it applies to them. Children know that personal information is as valuable online as offline and that it should not be shared without a parent, career or teacher's permission. Discuss with children, school rules for using the Internet.	**Hectors World Resources** Lesson 1- Personal Information **Think You Know Lee and Kim's Adventure** Lesson 1 Keeping Safe on the internet. **Online Resources** Smartie The Penguin story from KidSMART Early Surfers
Online Research	Children understand that they can find a range of information on the internet. Children are able to navigate age-appropriate websites. Children know what to do if they find something inappropriate online.	Use simple navigation skills to open a teacher selected website from a bookmarked link or shortcut. Make choices by clicking on buttons in a webpage and navigate between pages by using the forward and back arrows. Start to evaluate web sites by giving opinions about preferred or most useful sites. Know how to return to the home page of a teacher directed website. Know how to use Hector Protector if they see something inappropriate on a website and then tell a trusted adult.	**Online Resources** Infant Encyclopaedia Poisson Rouge ICT Games Cbeebies games V & A Museum of Childhood
Communication & Collaboration	Children know that there are a variety of online tools that can be used to communicate with other people. Children begin to understand the importance of being kind and polite online.	Know that email is a method of sending and receiving messages through the Internet. Participate in the sending of class emails, or alternative messaging system, e.g. via the school's learning platform.	**Online Resources** Purple Mash 2 Email Program Sebastian Swan – visit Sebastian's blog and contact Sebastian Swan Discussion forums on DB Primary

Online Safety	Year 2
National Curriculum PoS Statement	• Use technology safely and respectfully, keeping personal information private. • Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Children develop awareness what is meant by personal information and understand that it is unique to them. Identify characteristics of people who are worthy of their trust.	Children are aware that not everyone they meet online is automatically trustworthy. Children understand that personal information is unique to them and should not be shared without a teacher or parent's permission. Children identify characteristics of people who are worthy of their trust.	**Hectors World Resources** Lesson 2 – not everyone is trustworthy Lesson 3 – assessing trustworthiness
Online Research	Children use the internet purposefully to answer specific questions. Children know that not everything they encounter on the internet is true.	Children explore a range of age-appropriate digital resources. Children to know that not everything they find online is accurate. Know that some websites contain advertisements (often embedded) and learn how to ignore them.	**Online Resources** Pick websites of your choice for research or uses these websites to aid research: www.bbc.co.uk/schools/famouspeople www.bbc.co.uk/schools/barnabybear/
Communication & Collaboration	Children know the difference between communicating via email and online in a discussion forum.	Children are able to send suitable and purposeful online messages, developing awareness of appropriate language to use. Children know that passwords help to keep information safe and secure and that they should not be shared. Children contribute to a class discussion forum.	**Online Resources** Digiduck's Big Decision e-book from Kidsmart Purple Mash 2 Email Program Discussion forums on DB Primary

Online Safety	Year 3

National Curriculum PoS Statement	• Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour. • Identify a range of ways to report concerns about content and contact. • Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Children develop awareness of online behaviours, in order to stay safe on the web. Children develop understanding of the rules in relation to safe use of the Internet.	Children understand that any personal information they put online can be seen and used by others. Develop awareness of relevant Online Safety issues, such as cyber-bullying. Children understand and abide by the school's AUP and know that it contains rules that exist in order to keep children safe online. Be specific in what is meant by personal information and why is should be kept private. Know that passwords keep information secure and that they should be kept private.	**Activity Ideas** Make an Internet Safety Poster Share the School AUP **Online Resources** Top Tips for Safe Surfing poster from LGFL "What should you keep Safe?"
Online Research	Children develop strategies for staying safe when searching for content whilst using the Internet. Children to use the Internet to attempt to distinguish between fact and fiction.	Use child-friendly search engines independently to find information through key words. Understand that the Internet contains fact, fiction and opinions and begin to distinguish between them.	**Online Resources** www.kidrex.org/ Children's search engine www.kidsclick.org Children's search engine "What is Reliable?" Inaccurate information online
Communication & Collaboration	Children understand and use a range of online communication tools, such as forums, email and polls in order to formulate, develop and exchange ideas.	Use a range of online communication tools, such as email, forums and polls. Know how to deal with unpleasant forms of electronic communication (save the message and speak to a trusted adult). Be able to discern when an email should or should not be opened.	Online Resources "What should you keep Accept?" Unsolicited emails and attachments

Online Safety	Year 4

National Curriculum PoS Statement	• Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour. • Identify a range of ways to report concerns about content and contact. • Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Understand and abide by the schools acceptable use policy. Children are aware of the need to develop a set of online protocols in order to stay safe online. Children develop awareness of relevant Online Safety issues.	Children understand and abide by the school AUP and aware of the implications of not following the rules. Children understand that a password can keep information secure and the need to keep it a secret.	**Activity Ideas** Make an Internet Safety Poster Share the School AUP **Think You Know Cybercafe** Lesson Plan 1 – Using Technology to Communicate Lesson Plan 3 - 'Communication & Information'
Online Research	Children safely use the Internet for research and follow lines of enquiry. Children understand the function of a search engine and the importance of using correct search criteria. Children use the internet as a resource to support their work, and begin to understand plagiarism. Children know that not everything they find on the Internet is true.	Use internet search engines to gather resources for their own research work. Be aware of different search engines and discuss their various features (e.g. Google image & video search). Be aware that not everything they find online is accurate and that information needs to be checked and evaluated.	**Online Resources** Children's safe search engines: www.kidrex.org/ www.kidsclick.org www.primaryschoolict.com Spoof websites used to consolidate the concept that information isn't always reliable www.allaboutexplorers.com http://zapatopi.net/treeoctopus.html **Think You Know Cybercafe** Lesson Plan 5 - 'Responsible use of the internet'
Communication & Collaboration	Children use a range of communication tools to collaborate and exchange information with others, e.g. email, blog, forums. Children understand that the information they put online leaves a digital footprint or trail	Children use online communication tools to exchange and develop their ideas in a range of curriculum opportunities. Develop understanding of when it is unsafe to open an email or an email attachment.	**Online Resources** Purple Mash 2 Email Program Common sense – following digital trail http://www.commonsensemedia.org/educators/lesson/followdigital-trail-2-3 common sense – talking safely online activity 3 http://www.commonsensemedia.org/educators/lesson/talkingsafely-online-3-5 **Think You Know Cybercafe** Lesson Plan 4 - 'Using Email Safely'

Online Safety	Year 5

National Curriculum PoS Statement	• Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour. • Identify a range of ways to report concerns about content and contact. • Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Children understand the potential risks of providing personal information in an increasing range of online technologies both within and outside school.	Children recognise their own right to be protected from the inappropriate use of technology by others and the need to respect the rights of other users.	**Activity Ideas** Create a mind map: Risks relating to giving away to much private information **Online Resources** Where's Klaus Video- https://www.youtube.com/watch?v=i4GKXsAOYZE
Online Research	Children develop their online set of protocols in order to keep safe online. Children recognise inaccuracy and bias on the web and evaluate websites for their validity.	Children know that good online research involved interpreting information, rather than copying. Children are able to carry out more refined web searches by using key words. Children evaluate search results and refine as necessary for the best results. Know that information found on websites may be inaccurate or biased and to check the validity of a website. Children use websites where resources can be downloaded without infringing copyright. Acknowledge sources used in their work.	**Online Resources** For copyright free pictures and music; NEN Gallery, Audio Networks **Activity Ideas** Safe Searching lesson and Powerpoint **Our Online World LGFL** Boggle' activity –web research and making decisions about quality and accuracy of searched information. 'Bug catcher' activity to identify and stop unwanted security threats like viruses and malware and begin to understand threats.
Communication & Collaboration	Children use online tools to exchange information and collaborate with others within and beyond their school and begin to evaluate their effectiveness.	Be aware of the different forms of technology that can be used to access the Internet and communicate with others.	**Think You Know Cybercafe** Lesson 6- Chatting with care Lesson 8- Behaving responsibly

Online Safety	Year 6
National Curriculum PoS Statement	• Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour. • Identify a range of ways to report concerns about content and contact. • Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

	Learning Objectives:	Teaching Points:	Possible Resources:
E-awareness	Be aware of the risks of cyberbullying Evaluate their use of technology including the use of email, social networking, online gaming and mobile phones and consider how they present themselves online.	Be aware of the issues surrounding cyberbullying and understanding the impact on an individual of sending or uploading unkind or inappropriate content. Know that malicious adults use the Internet and attempt to make contact with children and know how to report abuse.	**Online Resources** "Let's fight it together", Cyberbullying section, accompanied by comprehensive teaching resources and video : http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx **Activity Idea** Poster to show the different types of technology available Poster about cyberbullying **Think You Know Cybercafe** Lesson 9- Social Networking Safe Profilling
Online Research	Children confidently and competently use the Internet as a tool for research and critically evaluate websites for their use. Children know that not all information they find on the Internet is accurate or unbiased and develop strategies for identifying the origin of a website. Children are aware of copyright issues and know that not all resources they find on the Internet are legal to use or copy	Children use a range of sources to check the validity of a website. Children recognise that different viewpoints can be found on the web. They critically evaluate the information they use, and understand some of the potential dangers of not doing so. Children are aware of the issues of plagiarism, copyright and data protection in relation to their work.	**Our Online World LGFL** 'Megabyte'– activity dealing with downloading and checking sites are safe, reliable and appropriate to task. Whose tube activity' – activity dealing with ownership of material and copyright if creating online. **Activity Idea** Checking the Internet: sites to validate- document saved on system. Contains Spoof websites used to consolidate the concept that information isn't always reliable
Communication & Collaboration	Students consider that they may encounter online messages from other people can make them feel angry, hurt, sad, or fearful. They explore ways to handle cyberbullying and how to respond in the face of upsetting language online	Decide which online communication tool is the most appropriate to use for a particular purpose, Be aware of the risks of cyberbullying and online grooming.	**ThinkUKnow Cybercafe** Lesson Plan 7 'Using Text & Picture Messaging' Lesson Plan 8 'Behaving Responsibly' DLG **Online Resources** Cyberbullying: https://www.youtube.com/watch?v=ouzGDzV8zvQ Newsround Caught in the web: https://www.youtube.com/watch?v=kgCNGvL0g1g