	Name of School	**St Joseph’s RC School**
	Policy review Date	**October 2016**
	Date of next Review	**October 2017**
	Who reviewed this policy?	**SLT – Computing Coordinator**

Managing e-mail at this school

This school:

- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively with up to date account details of users.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils’ LGfL LondonMail e-mail accounts are intentionally ‘anonymised’ for their protection..
- Year R/1 pupils are introduced to principles of e-mail through the Visual Mail facility in the London MLE OR closed ‘simulation’ software.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and ‘netiquette’ of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, *named LA system;*
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Appendix 1 – further information

How will e-mail be managed?

E-mail is now an essential means of communication for staff in schools and everyday life. Directed use of regulated e-mail in schools can bring significant educational benefits, increases the ease of communication with parents and within the school community and facilitates local and international school projects. However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate.

Technology:

Spam, phishing and virus attachments are all potential risks to be considered. Filtering software must be used to stop unsuitable mail. LGfL's filtering provision is highly efficient in this respect, although it should be stressed that the technology only forms part of the protection strategy and should not be relied upon in isolation. Instead, it should be used alongside good classroom and supervisory practices, user education, and diligent individual behaviour.

Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. Schools in London have appropriate educational, filtered Internet-based e-mail options through the London Grid for Learning (LGfL).

- StaffMail – (owned and operated by LGfL, and accessible via LGfL USO accounts).
- LondonMail (for students) – provided by Microsoft and accessible via LGfL USO accounts
- Safemail = LondonMail with restrictions applied (typically aimed at Key Stage 2 in particular)
- Visualmail = an additional feature within the London MLE (Fronter) - (aimed at Key Stage 1)

StaffMail is available to staff and governors within LGfL connected schools and LAs. It has the full functionality of a Microsoft Exchange account. It is accessed with the users' Unified Sign On (USO).

LondonMail is an email solution, which is filtered for inappropriate language and unsolicited mail, designed for pupil use. It uses a common format for identity but at the same time appears anonymous. This means a pupil's school (and thus their age group, gender and location) are not identifiable. This conforms to current standards.
e.g. a pupil named John Smith would have the account of smitj001.123@lgflmail.net where the first three digit number is used to accommodate multiple instances of users with a similar name, and the second is the DfE code of the Local Authority.

Although this seems anonymous, because the account is linked to a LGfL sign-on database (USO) the account is always accountable and traceable.

Staff can be given a LondonMail account but this must only be used for teaching and learning purposes with pupils, and is generally only relevant for Key Stage 2 teachers. These accounts are always restricted to usage within the particular school's LondonMail user group.

SafeMail is LondonMail with 'rules' applied which offers further restrictions on who the email can be sent to or received from. It is suggested this is used with Key Stage 2 pupils.

Visualmail is a feature of the London MLE and is an internal mail restricted to your school's MLE environment. Additionally the London MLE provides a variety of alternative options for communications within a closed network other than email such as using the forum tools.

If you have a serious child protection issue using email you should refer this to your LA or other appropriate authority, (e.g. a child's disappearance may require investigative access).

Education:

Staff and pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's e-Safety and anti-bullying education programme.

In addition to the Visualmail feature in the London MLE, there are programs that can be used with the youngest pupils that 'simulate' an E-mail system. This provides a useful environment to teach the skills of sending and receiving an e-mail with or without an attachment to very young pupils.

Pupils need to understand good 'netiquette' style of writing, (this links to English) and appropriate e-mail behaviour. An e-Literacy and e-Safety scheme of work with associated links is available at http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Further information on LGfL email services is available at www.email.lgfl.net

Information Handling advice:
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx