

**ST JOSEPH'S CATHOLIC PRIMARY SCHOOL  
CRAYFORD**

**E-SAFETY POLICY**

**SUMMER 2016**

**To be reviewed: Summer 2018  
Teaching and Learning  
Mr Clarke**

## **Mission Statement**

**The teachers and governors of St. Joseph's provide a broad, balanced curriculum to enable each child to achieve the highest standards of education in a Catholic ethos.**

### **THE AIMS OF ST JOSEPH'S CATHOLIC PRIMARY SCHOOL ARE:**

- to nurture the uniqueness of each individual as a member of God's family
- to ensure that the Catholic faith is at the heart of the whole school experience
- to create a well ordered supportive environment in an atmosphere conducive to learning where every child feels confident and safe.
- to create an atmosphere of reconciliation, where pupils can accept the consequences of their own actions, and be encouraged to make more responsible future choices
- to deliver a relevant curriculum with equal access for all pupils
- to encourage and support each child to achieve the highest standards of which they are capable
- to encourage each child to become a concerned compassionate member of society determined to promote justice and peace
- to promote good working relationships based on mutual cooperation and trust
- to provide a welcoming place for parents
- to work in harmony with the parish and the local community.

## **Contents**

1. Introduction and Overview
  - \* Rationale and Scope
  - \* Roles and responsibilities
  - \* How the policy be communicated to staff/pupils/community
  - \* Handling complaints
  - \* Review and Monitoring
2. Education and Curriculum
  - \* Pupil e-safety curriculum
  - \* Staff and governor training
  - \* Parent awareness and training
3. Expected Conduct and Incident Management
4. Managing the ICT Infrastructure
  - \* Internet access, security (virus protection) and filtering
  - \* Network management (user access, backup, curriculum and admin)
  - \* Passwords policy
  - \* E-mail
  - \* School website
  - \* Learning platform
  - \* Social networking
  - \* Video Conferencing
5. Data Security
  - \* Management Information System access
  - \* Data transfer
6. Equipment and Digital Content
  - \* Personal mobile phones and devices
  - \* Digital images and video
  - \* Asset disposal

## **Appendices:**

1. E-Safety/Personal Use of Social Media/Acceptable Use Agreement (Staff)
2. E-Safety Rules for Children
3. Home/School Agreement
4. E-Safety Permission for signature by parents
5. E-Safety Guidelines for Parents
6. Protocol for responding to e-safety incidents  
<http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx> - handling infringements
7. Search and Confiscation guidance from DfE  
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

## 1. Introduction and Overview

### **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/or 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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 (including 'frape' (hacking Facebook profiles)) 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 (Internet 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)

## Scope (from SWGfL)

This policy applies to all members of St Joseph's Catholic Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Joseph's Catholic Primary School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school / academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school / academy 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 e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"><li>* To take overall responsibility for e-safety provision</li><li>* To take overall responsibility for data and data security (SIRO)</li><li>* To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL</li><li>* To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant</li><li>* To be aware of procedures to be followed in the event of a serious e-safety incident.</li><li>* To receive regular monitoring reports from the E-Safety Co-ordinator</li><li>* To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)</li></ul>

Role	Key Responsibilities
E-Safety Co-ordinator / Designated Child Protection Lead	<ul style="list-style-type: none"> <li>* Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents</li> <li>* Promotes an awareness and commitment to e-safeguarding throughout the school community</li> <li>* Ensures that e-safety education is embedded across the curriculum</li> <li>* Liaises with school ICT technical staff</li> <li>* To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs</li> <li>* To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</li> <li>* To ensure that an e-safety incident log is kept up to date</li> <li>* Facilitates training and advice for all staff</li> <li>* Liaises with the Local Authority and relevant agencies</li> <li>* Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> <li>• sharing of personal data</li> <li>• access to illegal / inappropriate materials</li> <li>• inappropriate on-line contact with adults / strangers</li> <li>• potential or actual incidents of grooming</li> <li>• cyber-bullying and use of social media</li> </ul> </li> </ul>
Governors / E-safety governor	<ul style="list-style-type: none"> <li>* To ensure that the school follows all current e-safety advice to keep the children and staff safe</li> <li>* To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor</li> <li>* To support the school in encouraging parents and the wider community to become engaged in e-safety activities</li> <li>* The role of the E-Safety Governor will include: <ul style="list-style-type: none"> <li>• regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs )</li> </ul> </li> </ul>
Computing Curriculum Leader	<ul style="list-style-type: none"> <li>* To oversee the delivery of the e-safety element of the Computing curriculum</li> <li>* To liaise with the e-safety coordinator regularly</li> </ul>

Role	Key Responsibilities
Network Manager/technician	<ul style="list-style-type: none"> <li>* To report any e-safety related issues that arises, to the e-safety coordinator.</li> <li>* To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>* To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)</li> <li>* To ensure the security of the school ICT system</li> <li>* To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>* The school's policy on web filtering is applied and updated on a regular basis</li> <li>* LGfL is informed of issues relating to the filtering applied by the Grid</li> <li>* That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant</li> <li>* that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction</li> <li>* To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>* To keep up-to-date documentation of the school's e-security and technical procedures</li> </ul>
Data Assessment Co-ordinator	<ul style="list-style-type: none"> <li>* To ensure that all data held on pupils on the school office machines have appropriate access controls in place</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>* To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>* To embed e-safety issues in all aspects of the curriculum and other school activities</li> <li>* To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)</li> <li>* To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws (see Appendix 1)</li> </ul>

Role	Key Responsibilities
All staff	<ul style="list-style-type: none"> <li>* To read, understand and help promote the school's e-safety policies and guidance</li> <li>* To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy</li> <li>* To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices</li> <li>* To report any suspected misuse or problem to the e-safety Co-ordinator</li> <li>* To maintain an awareness of current e-safety issues and guidance e.g. through CPD</li> <li>* To model safe, responsible and professional behaviours in their own use of technology</li> <li>* To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. (see Appendix 1)</li> </ul>
Pupils	<ul style="list-style-type: none"> <li>* Read, understand, sign and adhere to the E-Safety Rules for Pupils (see Appendix 2)</li> <li>* Home/School Agreement is signed by parents when their child starts school(See Appendix 3)</li> <li>* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>* to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>* to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>* to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>* To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>* To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school</li> <li>* To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> <li>* to help the school in the creation/ review of e-safety policies</li> </ul>

Role	Key Responsibilities
Parents/carers	<ul style="list-style-type: none"> <li>* To support the school in promoting e-safety and endorse the Home/School Agreement (Appendix 3), E-Safety Permission (Appendix 4), E-Safety Guidelines (Appendix 5) which includes the pupils' use of the Internet and the school's use of photographic and video images</li> <li>* to access the school website</li> <li>* Acceptable Use Agreement.</li> <li>* to consult with the school if they have any concerns about their children's use of technology</li> </ul>
External groups	<ul style="list-style-type: none"> <li>* Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school</li> </ul>

### Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- \* Policy to be posted on the school website and in the staffroom policy folder
- \* Policy to be part of school induction pack for new staff
- \* Acceptable use agreements discussed with pupils at the start of each year.
- \* Acceptable use agreements to be issued to whole school community, usually on entry to the school
- \* Acceptable use agreements to be held in pupil and personnel files

### Handling complaints:

- \* The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- \* Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by E-Safety Coordinator / Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period
  - referral to LA / Police.
- \* Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- \* Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

## **Review and Monitoring**

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies

- \* The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- \* The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- \* The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- \* There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

## **2. Education and Curriculum - Pupil e-safety curriculum**

This school

- \* Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - To STOP and THINK before they CLICK
  - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - To know how to narrow down or refine a search;
  - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - To understand why they must not post pictures or videos of others without their permission;
  - To know not to download any files – such as music files - without permission;
  - To have strategies for dealing with receipt of inappropriate materials;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- \* Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- \* Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- \* Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- \* Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- \* Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

### **Staff and governor training**

This school

- \* Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection. The Office Manager will organise the encryption of data when required;
- \* Makes regular training available to staff on e-safety issues and the school's e-safety education program; annual updates/ termly staff meetings etc.
- \* Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

### **Parent awareness and training**

This school

- \* Runs a rolling programme of advice, guidance and training for parents, including:
  - Distribution of E-Safety Guidelines for parents
  - Information leaflets; in school newsletters; on the school web site;
  - Demonstrations, practical sessions held at school;
  - Suggestions for safe Internet use at home;
  - Provision of information about national support sites for parents.

### **3. Expected Conduct and Incident management**

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policies which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Students/Pupils
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

### **Incident Management**

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

#### **4. Managing the ICT infrastructure**

\* Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment.

- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search,
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator / teacher / person responsible for URL filtering]. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

#### Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users - the London USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- \* Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different / use the same username and password for access to our school's network;
- \* Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- \* We provide pupils with an individual network log-in username.
- \* All pupils have their own unique username which gives them access to the Internet;
- \* We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- \* Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- \* Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- \* Requires all users to always log off when they have finished working or are leaving the computer unattended;
- \* Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- \* Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at the end of the school day to save energy;
- \* Has set-up the network so that users cannot download executable files / programmes;
- \* Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- \* Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- \* Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- \* Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- \* Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- \* Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by IT Technician; equipment installed and checked by approved Suppliers / electrical engineers
- \* Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;  
e.g. teachers access report writing module; SEN coordinator - SEN data;

- \* Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems: e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- \* Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- \* Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- \* Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- \* Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements;
- \* Uses our broadband network for our CCTV system and have had set-up by approved partners;
- \* Uses the DfE secure s2s website for all CTF files sent to other schools;
- \* Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- \* Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- \* Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- \* All computer equipment is installed professionally and meets health and safety standards;
- \* Projectors are maintained so that the quality of presentation remains high;
- \* Reviews the school ICT systems regularly with regard to health and safety and security.

### **Password policy**

- \* This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- \* All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- \* We require staff to use <STRONG passwords for access into our MIS system>.
- \* We require staff to change their passwords into the MIS, LGfL USO admin site, <other secure system> twice a year.

## E-mail

This school

- \* Provides staff with an email account for their professional use, London Staffmail / LA email and makes clear personal email should be through a separate account;
- \* Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils; Uses Londonmail with students as this has email content control
- \* Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example [info@schoolname.la.sch.uk](mailto:info@schoolname.la.sch.uk) / [head@schoolname.la.sch.uk](mailto: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.
- \* Will ensure that email accounts are maintained and up to date
- \* 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..
- \* Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- \* 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 or 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.

\* Parents sign on behalf of pupils 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.

### **School website**

The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- Uploading of information is restricted to our website authorisers: <e.g. Office Manager and Teaching Assistant responsible for the website.
- The school web site complies with the statutory DfE guidelines for publications;

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;
  - Photographs published on the web do not have full names attached;
  - We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
  - We do not use embedded geodata in respect of stored images
  - We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

## **Learning platform – the school does not have a learning platform**

### **Social networking**

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.
- School staff will ensure that in private use:
  - \* No reference should be made in social media to students / pupils, parents / carers or school staff
  - \* They do not engage in online discussion on personal matters relating to members of the school community
  - \* Personal opinions should not be attributed to the school /academy or local authority
  - \* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## Video Conferencing

This school:

Only uses the LGfL supported services for video conferencing activity;

Only uses approved or checked webcam sites; CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety.

We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

## 5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- \* The Head Teacher is the Senior Information Risk Officer (SIRO).
- \* Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners <in a spreadsheet>.
- \* We ensure staff know who to report any incidents where data protection may have been compromised.
- \* All staff are DBS checked and records are held in one central record <in name of MIS e.g. SIMS, Progresso etc., Personnel or spreadsheet>.
- \* We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - Staff,
  - Governors,
  - Pupils
  - Parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- \* We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- \* We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- \* School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

- \* We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

## Technical Solutions

- \* Staff have <secure area(s) on the network to store sensitive documents or photographs>.
- \* We require staff to log-out of systems when leaving their computer, but also enforce lock-out after <10 minutes idle time>.
- \* We use <encrypted flash drives> if any member of staff has to take any sensitive information off site.
- \* We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- \* We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- \* Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- \* We use <RAv3 / VPN solution> with its 2-factor authentication for remote access into our systems.
- \* We use <LGfL's USO FX> to transfer other data to schools in London, such as references, reports of children.
- \* We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- \* We store any Protect and Restricted written material in <lockable storage cabinets in a lockable storage area>.
- \* All servers are <in lockable locations and> managed by DBS-checked staff.
- \* We <lock any back-up tapes in a secure, fire-proof cabinet>. <Back-ups are encrypted>. <No back-up tapes leave the site on mobile devices.>
- \* We use < LGfL's GridStore remote secure back-up / named alternative solution> for disaster recovery on our <network / admin, curriculum server(s)>.
- \* We comply with <the WEEE directive on equipment disposal> by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and <get a certificate of secure deletion for any server that once contained personal data>.
- \* Portable equipment loaned by the school (for use by staff at home), where used for any protected data, <is disposed of through the same procedure>.
- \* Paper based sensitive information is <shredded, using cross cut shredder / collected by secure data disposal service>.

## 6. Equipment and Digital Content

### Personal mobile phones and mobile devices

- \* The use of mobile phones are not permitted in the presence of children except in emergency situations. Pupils should be unaware of staff mobile phone. These must be stored discretely.
- \* Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- \* Student mobile phones which are brought into school must have parent's permission and must handed in to the school office on arrival at school (Year 6 children only).

Staff members may use their phones during school break times when children are not present.

All visitors are requested to keep their phones on silent.

- \* The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- \* The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- \* Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- \* Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- \* Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- \* Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets, during school swimming lessons.
- \* Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- \* The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- \* Personal mobile phones will only be used during lessons with permission from the teacher.
- \* No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- \* All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Students' use of personal devices

- \* The School strongly advises that student mobile phones should not be brought into school.
- \* The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- \* If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

- \* Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- \* If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- \* Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- \* Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.
- \* No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

#### Staff use of personal devices

- \* Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- \* Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- \* Staff will be issued with a school phone where contact with students, parents or carers is required.
- \* Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- \* If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- \* Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- \* If a member of staff breaches the school policy then disciplinary action may be taken.
- \* Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

## Digital images and video

In this school:

- \* 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;
- \* We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- \* Staff sign the school's E-Safety/Personal Use of Social Media Rules for Staff/Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- \* If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- \* The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- \* Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- \* Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- \* 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 identity 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.

## Asset disposal

Details of all school-owned hardware over £100 will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

**Signed:**        **Mr M Lawrence**  
                      **Chair of Governors**

**Date: 23/06/2016**

## **ST JOSEPH'S CATHOLIC PRIMARY SCHOOL E-SAFETY/PERSONAL USE OF SOCIAL MEDIA RULES FOR STAFF**

The computer system is owned by the school. The E-Safety rules help to protect staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of Internet access.
- School computer and Internet use must be appropriate to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the Head Teacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

### **Personal use of social media**

- School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at St Joseph's Catholic Primary School.
- Any communication received from children on any personal social media sites must be reported to the Designated Person for Child Protection.

- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported to the Head Teacher/Designated Teacher.
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business except in the case of an emergency.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.
- Staff should not accept any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Staff mobile phones must be stored discretely and must not be used in the presence of children except in the case of an emergency.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read and understood the rules for E-Safety/Personal Use of Social Media

Name: .....

Signed: .....

Date.....

## **ST JOSEPH'S CATHOLIC PRIMARY SCHOOL**

### **E-SAFETY RULES**

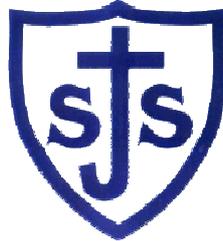
#### **Rules for Pupils** **Think then Click**

These rules help us to be fair to others and keep everyone safe.

- I will only use the internet when a member of staff is in the room and has given me permission.
- I will only look at or delete my own files.
- I understand that I must not bring software or memory sticks into school without permission.
- I will only e-mail people if my teacher or another staff member has approved.
- The messages I send will be polite and sensible
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will not open e-mails sent by anyone I don't know.
- I will not use Internet chat rooms
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher or other member of staff immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites. The school may also intercept e-mail and delete inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

# ST JOSEPH'S CATHOLIC SCHOOL AGREEMENT



## ***THE PARENTS***

### **I/We shall try to:**

- Support the religious ethos of the school;
- See that my child attends school regularly, arrives on time, wears the correct uniform and is properly equipped;
- Let the school know any concerns or problems that might affect my child's work or behaviour;
- Support the school's policies and guidelines on pupil behaviour;
- Support my child in homework and other opportunities for home learning;
- Read regularly with my child and keep teachers informed through the home/school reading record;
- Attend Parents' Evenings and discussions about my child's progress;
- Take an interest in my child's life at school.
- I agree that any photographs, video recording taken at school events will be for personal use only and will not be uploaded onto any Social Media site.
- I agree not to damage the reputation of St Joseph's Catholic Primary School by making inappropriate comments on Social Networking sites.
- I agree that my child will not bring into school mobile phones without the permission of the school (Year 6 pupils only) and that such mobile devices will be kept secure in the school office.
- I agree to monitor the use of my child's internet, social media networking

sites, ensuring that inappropriate messages are not sent or received.

## ***THE SCHOOL***

### **St Joseph's will:**

- Involve parents in liturgical and religious events;
- Contact parents if there is a problem with attendance, punctuality, uniform or equipment.
- Keep parents informed of their child's progress, including a written annual report;
- Set, mark, monitor homework;
- Arrange Parent's Evenings during which progress will be assessed;
- Keep parents informed about school activities through regular letters home, newsletters and notices about special events.

**Signed:** ..... (Parents)

**Parent/Guardian of** ..... **Please print.**

**Signed:** ..... (Head Teacher)

## ST JOSEPH'S CATHOLIC PRIMARY SCHOOL

### E-SAFETY PERMISSION

Please complete, sign and return to the School Office.	
<b>Pupil:</b>	<b>Class:</b>
<b>Parent's Consent for Access to Internet technologies</b> I have read and understood the school rules for e-safety and give permission for my son / daughter to continue to access Internet technologies. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of Internet technologies.	
<b>Signed:</b>	<b>Date:</b>
<b>Please print name:</b>	
<b>Parent's Consent for Web Publication of Work and Photographs</b> I agree that, if selected, my son / daughter's work may be published on the school Website. I also agree that photographs that include my son / daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.	
<b>Signed:</b>	<b>Date:</b>

Copies of the e-safety policy are available from the office on request.

## **E-SAFETY GUIDELINES FOR PARENTS / GUARDIANS**

Consider some of the points below to ensure that your child is using the fantastic new technologies available to them as safely as possible.

1. Please consider employing the strict "safe search" setting on Google.  
For more information on this and further guides you could look at [www.candp-s.com/familysafety](http://www.candp-s.com/familysafety) - a website full of useful material and advice on Online Safety.
2. Look into setting Parental Controls on a Windows 10, Windows Vista, Windows 7 or Mac computer to restrict specific web sites and also the time when the computer can be used.
3. Mobile phones offer children an amazing amount of opportunity in what they look at and what they can text, including picture messaging. If your child has a smart phone, then please consider setting safe searches on Google and YouTube on these as well.
4. Please take time to talk to your child about their use of the internet. It will be impossible and perhaps not even desirable to ban everything; indeed they are often much more able than us at using the computer! Education and dialogue are the only realistic ways to protect young people.
5. Please encourage a balanced use of the computer and mobile phones- for example, setting expectations that computers are off at 10pm and phones aren't used at mealtimes or ½ hour before bedtime (and not once in bed!).

### **\*How a parent/carer can ensure that their child's online experience is safe.**

1. **Learn** - Find out more about online threats
2. **Talk** - Discuss what your child should, and should not, do online and print off a copy of the Safe Internet Use Agreement - sign it and put it on the wall.
3. **Have fun** - Enjoy some of the recommended sites by going online together (let your child show you how).
4. **Take action** - Make searching on the internet safer by blocking pornography on Google and YouTube and get a healthy balance by setting time restrictions on your child's computer.
5. **Care** - Make each child's computer use more comfortable – avoid posture problems by getting a laptop riser and separate keyboard and mouse and finally – encourage each child to learn to type.

## Appendix 6

### Policy: How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

<b>STUDENT</b>	
<b>Category A infringements</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Use of non-educational sites during lessons</li> <li>• Unauthorised use of email</li> <li>• Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends</li> <li>• Use of unauthorised instant messaging / social networking sites</li> </ul>	<p><b>Refer to class teacher / tutor</b></p> <p>Escalate to: senior manager / e-Safety Coordinator</p>
<b>Category B infringements</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Continued use of non-educational sites during lessons after being warned</li> <li>• Continued unauthorised use of email after being warned</li> <li>• Continued unauthorised use of mobile phone (or other new technologies) after being warned</li> <li>• Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups</li> <li>• Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc</li> <li>• Trying to buy items over online</li> <li>• Accidentally corrupting or destroying others' data without notifying a member of staff of it</li> <li>• Accidentally accessing offensive material and not logging off or notifying a member of staff of it</li> </ul>	<p><b>Refer to Class teacher/ Head of Department / Year tutor / e-safety Coordinator</b></p> <p>Escalate to:</p> <p>removal of Internet access rights for a period / removal of phone until end of day / contact with parent]</p>

<b>STUDENT</b>	
<b>Category C infringements</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site.</li> <li>• Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)</li> <li>• Trying to access offensive or pornographic material (one-off)</li> <li>• Purchasing or ordering of items online</li> <li>• Transmission of commercial or advertising material</li> </ul>	<p><b>Refer to Class teacher / Year Tutor / e-safety Coordinator / Head teacher / removal of Internet and/or Learning Platform access rights for a period</b></p> <p>Escalate to: contact with parents / removal of equipment</p> <p><b>Other safeguarding actions if inappropriate web material is accessed:</b> Ensure appropriate technical support filters the site</p>
<b>Category D infringements</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned</li> <li>• Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent</li> <li>• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988</li> <li>• Bringing the school name into disrepute</li> </ul>	<p><b>Refer to Head Teacher / Contact with parents</b></p> <p><b>Other possible safeguarding actions:</b></p> <ul style="list-style-type: none"> <li>• Secure and preserve any evidence</li> <li>• Inform the sender's e-mail service provider.</li> <li>• Liaise with relevant service providers/ instigators of the offending material to remove</li> <li>• Report to Police / CEOP where child abuse or illegal activity is suspected</li> </ul>

<b>STAFF</b>	
<b>Category A infringements (Misconduct)</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.</li> <li>• Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.</li> <li>• Not implementing appropriate safeguarding procedures.</li> <li>• Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community.</li> <li>• Misuse of first level data security, e.g. wrongful use of passwords.</li> <li>• Breaching copyright or license e.g. installing unlicensed software on network.</li> </ul>	<p><b>Referred to line manager / Head teacher</b></p> <p>Escalate to:</p> <p><i>Warning given</i></p>
<b>Category B infringements (Gross Misconduct)</b>	<b>Possible Sanctions:</b>
<ul style="list-style-type: none"> <li>• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;</li> <li>• Any deliberate attempt to breach data protection or computer security rules;</li> <li>• Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;</li> <li>• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;</li> <li>• Bringing the school name into disrepute</li> </ul>	<p><b>Referred to Head teacher / Governors;</b></p> <p><b>Other safeguarding actions:</b></p> <ul style="list-style-type: none"> <li>▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.</li> <li>▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.</li> <li>▪ Identify the precise details of the material.</li> </ul> <p><i>Escalate to:</i></p> <p><i>report to LA /LSCB, Personnel, Human resource.</i></p> <p>Report to Police / CEOP where child abuse or illegal activity is suspected. ,</p>

### **If a member of staff commits an exceptionally serious act of gross misconduct**

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

### **Child abuse images found**

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

[http://www.ceop.gov.uk/reporting\\_abuse.html](http://www.ceop.gov.uk/reporting_abuse.html)

<http://www.iwf.org.uk>

### **How will staff and students be informed of these procedures?**

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use agreement form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see LGfL safety site).

