

Our Lady of Peace Catholic Primary and Nursery School

'With Christ in our hearts, together we grow'.



Computing Code of Conduct – On-line Safety, Social Media & Computing Systems

By order of the Governing Body of Our Lady of Peace Catholic Primary and Nursery School

This policy was implemented April 2016

E Safety Officer: Headteacher

Scope of the policy

This policy applies to all members of the school community (including but not limited to pupils, staff, governors, parents, volunteers, students, PTA) who have access to and are users of school ICT systems, both in and out of the school. It also applies to members of the school who access the internet and social media away from the school's premises.

It sets out to:

- assist those working with pupils to work safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils
- offer a code of practice relevant to social media for educational, personal and recreational use
- advise that in the event of unsafe and/or unacceptable behaviour disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with pupils and takes account of the variety of legislation appropriate to this policy.

Teaching and Learning

Why is use of the Internet so important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

What are the benefits of using the Internet for the education of our children?

- access to world-wide educational resources (with strict filtering procedures);
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional organisations and colleagues;
- improved access to technical support including remote management of networks and
- exchange of curriculum and administrative data at both local and national government levels.

How will Internet use enhance the learning of pupils?

- the school Internet access, through pupil logins, will be designed expressly for pupil use and will include appropriate filtering;
- pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use and
- pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (In practice monitoring may be delegated to appropriate members of staff.)

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the Web site particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs are taken of children.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Internet Service Provider via the ICT Co-ordinator or e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Internet access will be blocked for access by pupils and websites which are deemed suitable for children will be added to a 'safe' list.

Internet Code of Conduct

- Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals. The internet is not necessarily secure and school sensitive information could be viewed by unauthorised individuals.
- The transmission of school sensitive data over the internet is strictly prohibited.
- At no time may staff use the Internet to send school or personal information that would be, if intercepted, place the school in violation of UK laws or regulations.
- Staff may not use the Internet to view illegal, pornographic or seditious material that would place the school at legal risk.
- Staff may not download or distribute material from the Internet without virus checking. Users are responsible for virus checking any material that may be forwarded.

- Staff may not use the Internet in a role inconsistent with their role in the school.
- Staff may not use the Internet for private business purposes or private commercial gain.
- Staff must read and agree to the E Safety and Social Media Policy regarding use of social media sites and communication with parents.

Managing Technologies

Technology

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- *Mobile phones will not be used during lessons or formal school time.* Mobile phones should not be used to take photographs, they should be locked away. The sending of abusive or inappropriate text messages is forbidden.
- Staff should not use personal mobile phones to contact pupils or parents and should keep any communications transparent and on a professional basis, for example by using professional email addresses. Where there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of the senior management team should be made aware and will decide how to deal with the situation.

School Computing Systems

- Staff must understand that school ICT systems may not be used for private purposes without specific permission from the head teacher.
- Staff must appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- Staff must understand that use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- Staff will respect system security and will not disclose any password or security information to anyone other than an authorised system manager.
- Staff will not install any software or hardware without permission.
- Staff will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Staff will respect copyright and intellectual property rights.
- Staff will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Co-ordinator or Headteacher.
- Staff will promote e-safety within the guidelines of the E Safety and Social Media Policy.

Passwords and Transferring/Sending/Storing Data

- Passwords for emails/logins/SIMs should not be shared with anyone (unless for PPA teachers).
- Information and data shared with external agencies should be encrypted with a password before being emailed.
- Information shared between staff and outside agencies should only be done so using a professional email account. This is including, but not limited to, staff meeting minutes, data, planning and any other information to do with school.

- Data that includes childrens' personal information such as surnames, levels and dates of birth should only be stored on an encrypted memory stick, or the school server. Data which does not identify individuals may be stored on a non-encrypted memory stick where an encrypted one is not available.

Emails

- The computer resources at Our Lady of Peace Catholic Primary and Nursery School belong to the school and are to be used solely for education or business purposes, although the Governors will permit limited use for personal purposes, provided that it does not interfere with work performance and provided that rules of usage are observed. This also applies to personal equipment being used on school site.
- Care should be taken if using e-mail to send or forward any personal attachments to external e-mail addresses. Documents of a sensitive nature should be password encrypted. Email subject lines should not contain the full name, or DOB, of any child.
- If any attachments are received with a personal e-mail they should be forwarded to the individual unless permission is obtained to download them.
- Only licensed software is in use in school. Under no circumstances must copyright or licensing requirements be breached.
- Business documents attached to e-mails received can be opened and saved to the network but they may be subject to copyright rules and extreme care must be taken when doing so. Similarly documents can be sent as attachments following the same rules.
- As some e-mail viruses spread so quickly no virus checking software can detect all attachment viruses quickly enough so if you have any doubts at all about the origin, or validity, of an attachment do not open it without checking internally with the system manager and with the sender.

The school realises that inbound e-mail may contain explicit and other unsuitable material beyond the control of the school. This should be immediately reported to the Computing Leader and Headteacher and marked as 'inappropriate' before deletion. The distribution, using any school resource, of an explicit material, chain letters, inappropriate humour, explicit language or offensive images is strictly forbidden.

The Headteacher / Computing Leader must be advised if any 'virus warnings' occur. Any downloads from the internet must be virus checked before use.

Do not allow anyone else to use your login ID and password or leave your computer on view when away from it. You could be held responsible for all inappropriate activity using your logon ID.

Employees cannot expect that any e-mail messages composed, received or sent on the school network, regardless of personal e-mail passwords, will be for private viewing only.

The school reserves the right to inspect the contents of any e-mail that is sent or received. If inappropriate use of e-mail is suspected the school reserves the right to investigate.

If in any doubt about the sensitivity included in an e-mail staff should refer to the Headteacher. Staff should take care in drafting e-mails so that they are done in a professional manner. They are a form of business correspondence and should be presented professionally.

Be aware of data protection issues and the use of personal data by which an individual may be identified.

Social Media

For the purposes of this policy, social media are interactive online media that allow parties to communicate instantly with one another or share information in a public forum. Examples include

- Social Networking sites such as Facebook, Bebo, MySpace and LinkedIn.
- ‘Blogging’ (written personal journals to publicly accessible internet pages)
- Video- and image-sharing websites such as YouTube, Instagram and Flickr.
- ‘Microblogging’ applications such as Twitter
- MSN
- Virtual worlds
- Media sharing
- Online discussion forums

Staff should be aware that there are many more examples of social media and this is a constantly developing area of communication. Employees should follow these guidelines in relation to any social media that they use, both at work and in their personal situation.

Use of Social Media in the School

Staff are not permitted to access social media websites from the school’s computers or other devices at any time unless authorised to do so by a member of the senior management team. They may, however, use their own computers or other devices while they are in the school to access social media websites outside of school session times, but excessive use of social media which could be considered to interfere with productivity will be considered a disciplinary matter.

Mobile phones should be switched off during school session times (working hours) and locked away. In the case of personal emergencies staff must see the Headteacher to request permission to have access to their mobile phones during working hours.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute
- Breach confidentiality
- Breach copyrights of any kind
- Bully, harass or be discriminatory in any way
- Be defamatory or derogatory

Use of Social Media outside the School

The school appreciates that people will make use of social media in a personal capacity but they must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to damage the reputation of the school, so a statement such as “the opinions expressed here do not necessarily reflect those of my employer” should be clearly stated and it is advisable to omit any references mentioning the school by name or the person by job title.

Opinions should, in any case follow the guidelines above to not bring the school into disrepute, breach confidentiality, breach copyrights or bully, harass or discriminate in any way.

Staff, governors, students, volunteers and parents of children attending the school should adhere to the following:

- Pictures and videos of any children, who are not their own, should not be posted onto ANY website; including, but not limited to, those mentioned at the beginning of the document.
- Pictures and videos of staff should not be posted to social media sites without prior consent.
- Individuals should not 'tag' themselves at the location of the school and should not mention the school's name in any location services provided by social media.
- The school's name should not be mentioned in any 'statuses', 'tags', 'tweets' or any other similar outlets within social media.
- Professional opinions, issues, problems or any other means of expression regarding the school should not be published on social media.
- Do not discuss the school on any public forum including, but not limited to, social networking sites and blogs.
- Staff should not mention the school's name when listing places of work on social media.
- Staff should not comment on other people's social media outlets that make any reference to the school – positively or negatively.
- Do not befriend pupils or parents (unless already known in a social capacity before the children attended the school).
- Do not set up and use pages, profiles or accounts, in the school's name, online.
- Prior to joining the school new employees should check any information they have placed on social media sites and remove any statements that might cause embarrassment or offence.
- If any of the above is witnessed/seen on social media it should be reported to senior management immediately.
- Any breach of the above will result in a disciplinary procedure with any persons found to be involved.

General Considerations

When using social media staff and others should:

- never share work log-in details or passwords
- keep personal phone numbers private
- not give personal email addresses to pupils or parents
- restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and therefore are expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within the school and outside of it. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for "cyberbullying" for example or possibly identity theft. Staff should not make "friends" of pupils at the school as this could potentially be construed as "grooming", nor should they accept invitations to become a "friend" of any pupils.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource.
- The school will keep a record of all staff and pupils on Sims who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.
- Parents will be asked to sign and return a consent form.

Assessing risks

- In common with other media such as magazines, books, videos and DVDs, some material available via the Internet is unsuitable for our pupils. The school will take all reasonable precautions to ensure that users access only appropriate material; including ‘allowing’ only ‘safe’ sites to be accessed from pupil logins. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Slough Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Communicating the Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents’ support

- Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Laptop Computers

Laptops which are the property of the school fall under the same restrictions of use as networked computers. Serious misuse of Laptops will be treated as a disciplinary offence and may result in dismissal. Loss, damage or theft of a Laptop through misuse, or negligence may result in financial sanctions.

Laptops and peripherals should be kept in a secure place and transported in the car boot.

Disciplinary Action

Any breaches of this policy, made by staff or governors, may lead to disciplinary action under the school's disciplinary Policy. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to dismissal.

Breaches of this policy made by parents will be taken up by the head teacher and, where deemed serious enough, may result in the exclusion of the child(ren).

I have read, understood and accept the Computing Code of Conduct, which includes: E - Safety, Social Media, Computing Systems, Use of Internet and Staff Code of Practice.

Name:

Signed:

Date:

Accepted for school: Headteacher