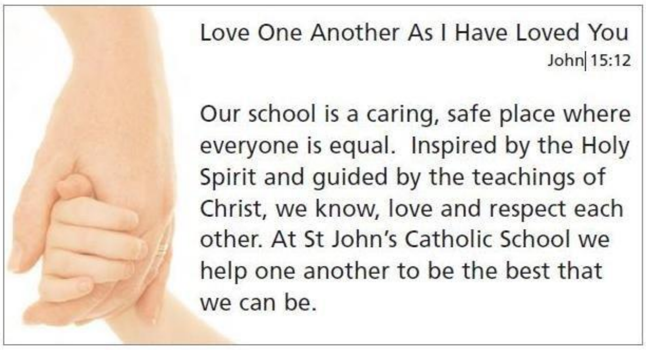

Love One Another As I Have Loved You

John 15:12

Our school is a caring, safe place where everyone is equal. Inspired by the Holy Spirit and guided by the teachings of Christ, we know, love and respect each other. At St John's Catholic School we help one another to be the best that we can be.

St John's Catholic Primary School
E Safety Policy 2016

Introduction

Our E-Safety Policy has been written by the school, building on the Oxfordshire ICT Development Service E-Safety Policy and government guidance. It has been agreed by the senior management and approved by Governors.

The E-Safety Policy will be reviewed annually or as new technologies emerge. There is a "whole school ownership" of the policy. It has been developed in consultation with a wide range of staff and pupils.

The E-Safety Policy covers the use of all ICT systems, equipment and software in school, including the internet, email, computers, laptops, tablets, cameras, mobile phones and other mobile technologies. It also addresses school related ICT out of school and the use of personal ICT equipment in school.

The school is committed to act on E-Safety incidents both inside and outside the school on issues that will affect the well being of staff and pupils. Incidents raising concerns about the safety of any children will be dealt with in accordance with the child protection policy. Staff development in safe and responsible internet use, information security and the school E Safety Policy will be provided as required.

Teaching and Learning

The Internet is an essential element in 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.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management of information and business administration systems.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the LA and DfES

How will pupils learn how to evaluate Internet content?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

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 Oxfordshire LA can accept liability for the material accessed, or any consequences of internet access.

Therefore pupils need to have input on how to evaluate information received. They also need to be taught what to do in case they are confronted with something distasteful/ unsuitable. Evaluation also needs to be made regarding the accuracy of the information they are looking at.
Pupils will be taught in E-Safety lessons and throughout other lessons to question the source of Internet information and its reliability.
Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
Pupils should be taught research techniques and key information handling skills and the evaluation of on-line materials is a part of every subject.
If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported and logged in the ICT book in the school office, and where appropriate the SLT.

Managing Information Services
The security of the school information systems will be reviewed regularly.
The school uses the Oxfordshire Broadband with its firewall and filters.
The school provides an additional level of protection through its deployment of Policy Central in partnership with Oxfordshire ICT Development Service.
We recognise that Information Management is a complex and multi-faceted set of processes. Information/ data held is a major responsibility which can have implications for the personal safety of staff and pupils. Effective information management requires a combination of robust technical systems and appropriate behaviour by the user. The most sophisticated information security system can be completely

undermined by the member of staff who leaves the system logged on and unattended whilst they are distracted by something. Therefore, security strategies will follow Oxfordshire LA guidelines. The security of the school information systems will be reviewed regularly and virus protection will be updated regularly.

Personal data sent over the Internet will be encrypted or otherwise secured. Staff will not use their personal email for school business.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 1998.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual).

The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

Passwords/Security

All pupils and staff have individual logins to ensure personal accountability and security. All staff have individual passwords and know to keep these secret.

How will email be managed?

To ensure safety, pupils may only use approved e-mail accounts on the school system and will adhere to our acceptable use agreement.

Pupils must immediately tell a teacher if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Use of words included in the filtering/checking 'banned' list will be detected and logged.

When using email to contact external organisations these should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will published content be managed?

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published. Photographs and video images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Staff will not take school cameras home. Staff will not take photos of children on their own personal devices. (e.g. phones and cameras)

How will social networking and personal publishing be managed?

All users will sign the Acceptable Use Agreement / E Safety Rules and blogging terms and conditions. (see these individual documents for detail)

Pupils will use the school website hosted by 123ICT as a safe way of emailing/video messaging/blogging/discussing.

Video conferencing is only to be used with a member of staff leading. Pupils will not be left unattended whilst using these technologies.

Written permission from parents/carers is needed before images (pictures and videos) of pupils are used.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, email address, names of friends etc.

How will filtering be managed?

The school will work in partnership with the Oxfordshire ICT Development Service, as well as 123ICT technicians to ensure filtering systems are as effective as possible.

If staff or pupils discover unsuitable sites, Oxfordshire ICT Development Service will contact the school and inform the head teacher.

In addition, staff will contact the Oxfordshire ICT Development Service and inform them of any unsuitable sites that need to be blocked. Details will also be logged in the E Safety Incident book in the staff room, and where appropriate the SLT informed.

How can emerging technologies be managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Personal mobile phones/hand held devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Pupils are not permitted to have mobile phones in school, with the exception of year 6 children who walk home on their own. In this circumstance a written letter of consent must be given to the head teacher, who then grants permission for the individual to have their mobile phone in case of emergency when walking home. Staff do not use or have on display their mobile phones when the children are present.

How should personal data be protected?

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

Policy Decisions

How will internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted Internet access. All users have individual log-ins to access the computers, with the exception of Early Years who share a class log on.

How will risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. 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 OCC can accept liability for the material accessed, or any consequences of Internet access.

If staff or pupils discover unsuitable sites, Oxfordshire ICT Development Service will contact the school and inform the head teacher. In addition, staff will contact Oxfordshire ICT Development Service and inform them of any unsuitable sites that need to be blocked.

All users must read and abide by the Acceptable Use Agreement which also asks that E-Safety rules be implemented in school and at home.

Pupils are educated about the risks of internet misuse through regular PHSE lessons and e-safety lessons.

Staff are aware that there may be spot checks on staff laptops at least once a year.

Cyber Bullying

Pupils in the school have Internet Safety lessons which discuss potential issues, including cyber bullying. Cyber Bullying is listed as unacceptable behaviour in the school's Behaviour Policy. The culture of the school encourages all members to report any misuse of ICT, including internet misuse. Pupils are encouraged to inform a member of staff if worried about any aspect of internet misuse or other ICT issues. In addition, all pupils have access to a "prayer/ worry box/ worry eater" in every classroom where they can write about any issues they wish to speak to the teacher about on a one to one basis. This includes e-safety concerns.

How will e-safety complaints be handled?

All E-Safety incidents will be logged in the E Safety Incident book in the staff room.

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 who should use the agreed OCC procedures. Any complaints referring to the Head Teacher must be referred to the Chair of Governors.

Sanctions

All pupils and staff are aware of the responsibilities they have when using the internet at school and home.

Pupils will be reminded of e-safety procedures every term as part of the ICT curriculum.

How is the internet used across the community?

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice. Each year e-safety is highlighted on internet safety day, where parents are also invited to an e-safety awareness talk delivered by one of the specialists from our 123 ICT team.

Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of St. John's RC Primary School at all times. Staff must sign the 'Staff Laptop and Computer Loans Agreement before taking the equipment away from the school premises.

Review January 2018

Staff Laptop and ICT Equipment Loan Agreement

I have borrowed a school laptop to use out of school in agreement with both Head Teacher and the ICT coordinator.

Make: ___________________________________

Model: ___________________________________

Serial number: ___________________________________

It is understood that I will return the equipment to school if requested to do so by either the Head Teacher or
the ICT co-ordinator.

I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.

I will use the equipment in accordance with the schools e-Safety Policy and Staff Acceptable Use policy.

I agree to the above conditions:

(Signature) ________________________________

(Print name) ________________________ Date:___________