St Gregory's Catholic Primary

E-Safety Policy for School Based Staff

Introduction

Children interact with new technologies such as mobile phones and the internet on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place children and young people in danger.

The issue of e-safety issues relating to children and young people and their safe use of the internet, mobile phones and other electronic communications, both in and out of school. It includes educating children on the risks and responsibilities of using such technologies safely and is part of the 'duty of care' which applies to everyone working with children.

This policy is one of the strategies the school uses to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

Who this policy is for

- This e-safety policy has been written by the school, building on government guidance and the advice of the Local Authority. It has been approved by governors and the school leadership team. This policy is available for staff.
- Advice on e safety is available on the pupil and governor portals.
- Parents have been made aware that the school has a policy on e-safety and are advised on ways of keeping their children safe at home. Further information on e-safety is available on Sandwell Together Learning Gateway.
- It is the responsibility of all staff to ensure that they use communications technology and the internet safely and responsibly. To this end all staff agree to an acceptable use policy (AUP)

  This policy is reviewed annually.

The Internet

The internet is now an essential part of the daily running of a school. The purpose of internet use at St Gregory's School is to:

- Raise educational standards
- Promote achievements
- Support the professional work of staff
- Enhance management systems
- Provide information to parents and the wider community

E-Safety actions

- The school's Internet access is designed for pupil use and includes filtering appropriate to the age of the children.
- Children are taught what internet use is acceptable and what is not and are given clear objectives for using the internet

- Children are taught how to use the internet effectively including how to locate, retrieve and evaluate relevant information, this ensures that they are less likely to discover sites containing inappropriate material.
- KS1 children are supervised when using the internet and will only access specific, approved on-line materials.
- Children are taught to evaluate the relevance, accuracy and quality of internet sourced material. Children report any unsuitable material found on the internet immediately to an adult.
- All staff report unsuitable material found on the internet immediately to the Head teacher
- Children are taught to acknowledge the source of information used and understand the importance of copyright laws
- Staff and children agree to and sign an Acceptable Use policy (AUP)

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school can not accept liability for the material accessed, or any consequences resulting from internet use.

Managing Information

System Security

It is important that a school reviews and maintains the security of the whole ICT system. This ensures the on-going delivery of essential learning services as well as the personal safety of staff and pupils. Maintaining ICT security is a major responsibility of a school. It is a complex matter and will not be coerced in full in this policy.

E-Safety Actions

- The security of the school's information systems is reviewed regularly by the Head Teacher and appropriate staff.
- Virus protection is updated regularly
- Use of the learning gateway ensures that all data sent by e-mail is secure
- Files held on the school's network are checked regularly and modified or deleted when necessary.

E-Mail

E-mail is an essential means of communication for both staff and pupils however the implications of e-mail use in school needs to be monitored. E-mails can be difficult to monitor but unregulated e-mail can leave pupils exposed to influences outside what is acceptable in school.

E-Safety Actions

- Children only use their Learning Gateway e-mails addresses.
- Children tell an adult immediately if they receive an offensive e-mail.
- Children do not reveal personal details about themselves or others in e-mails or arrange to meet with a specific person.
- Access to staff and children to personal e-mail accounts is blocked (eg Yahoo or hotmail)
- The forwarding of chain letters is nor permitted

Published Content

St Gregory's regularly publishes information, resources and children's outcomes on the school's management system, website and Office Portal. Personal information should only be held on secure systems which are accessed by authorized staff whereas general information about the school may be published wider. The Office Portal is the most effective way of publishing information relevant to the school, families and community as it requires authentication while reaching a wide and relevant audience, however, sometimes it is useful to use the website. In these cases consideration of personal and school security is essential.

E-Safety Actions

- The content details on the website are: school address, e-mail and telephone number. Staff or children's information is not shared.
- The Head teacher has overall editorial responsibility for the website to ensure that content is accurate and appropriate
- Parents or carers give written permission for images of children to be posted on the website, pupil and family portals unless individual children cannot be clearly identified.
- Work is only published with the permission of the child and their parent/carer.

Social Networking

Parents and staff need to be aware that the internet has online spaces and social networking sites which allow children to publish content (eg photos, comments and personal information). These sites are only viewed by invited 'friends'.

When used by responsible adults social networking sites provide easy to use free facilities however children should be encouraged to think about the issues relating to uploading personal information before signing up to social networking.

E-Safety Actions

- The school blocks access to social networking sites.
- Children are taught about the dangers (including bullying) of sharing personal information, especially on-line.
- Staff are not encouraged to use social networking sites and to be aware of the nature of what they are publishing on-line in relation to their professional position.
- If staff are signed up to social networking sites they are encouraged to use them only for social reasons and must not discuss any matters relating to the school, children or their professional role on-line.
- Staff do not invite children to be 'friends' on-line and equally do not accept requests for friendship from children or past pupils of the school.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tool, including mobile communications and multi media. A risk assessment needs to be undertaken on each new technology before using it with children. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

E-Safety Actions

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is permitted

- Children are not allowed to bring mobile phones to school. If phones are brought in they are handed in at the office and returned at the end of the day.
- Personal mobiles and digital cameras are not used to record sound and images during the school day (this includes school trips)
- All video conferencing is supervised by an adult.

Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be useful in improving services, data could be mishandled, stolen or misused. The data Protection Act 1998 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. The head teacher is responsible for ensuring the Data Protection procedures are in place.

E-Safety Actions

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

Contacts and References

Sandwell's Local Safeguarding Children's board
http://www.sandwellscb.org.uk/

Think You Know?
http://www.thinkyouknow.co.uk/

Child Exploitations and on-line Protection Centre
http://www.ceop.gov.uk/

Signed …M.O'Brien…… Chair of Governors

Date: February 2016