ST WALBURGA'S CATHOLIC PRIMARY SCHOOL

E-Safety Policy

Mission Statement:

At St Walburga's we celebrate that we are all members of God's loving family. We do our best to follow Jesus by putting others first. Our school is a happy and safe place where we learn, have fun together, do well and achieve our full potential.

This policy is to be read in conjunction with the Child Protection Policy, Staff ICT Acceptable Use Policy, Disciplinary Policy and ICT Policy.

To create a secure and safe environment which develops technology skills and provides pupils with awareness of potential E-Safeguarding scenarios that may arise.

Policy statement

New technologies have become integral to the lives of children and young people in today's society, both outside and within school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, improve Literacy and communication skills, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information

- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/Internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- The risk of being subject to grooming by those with whom they make contact on the Internet

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision to build pupils' awareness to the risks which they may be exposed, so that they have the confidence and understanding to seek advice and to deal with any risks in an appropriate manner.

The E-Safeguarding Committee

Our school has an E-Safeguarding committee which includes the following members:

Mrs E Snelling (Head Teacher, Designated Safeguarding Lead)
Mrs A Haines (Deputy Head, Designated Safeguarding Lead, E-Safeguarding Coordinator, Computing Leader)
Mr A McKniff (Teaching Assistant and School Council Leader) who will bring school council members to the meetings when applicable
Mrs N Mazeepa Specchia – Named Governor for E-safeguarding

Our school ICT technician is Andy Barker from Datacable. The committee will consult him regarding any technical issues related to the safeguarding and security of data.

The E-Safeguarding committee will meet termly to

- Discuss and review policies
- Discuss any E-Safety incidents recorded within the E-Safety log
- Discuss issues raised in E-Safety lessons
- Discuss cause for concerns relevant to E-safety through Child Protection procedures
- Discuss and review the progress being made against the school's E-Safeguarding action plan.

Meeting minutes will be recorded and filed within the Coordinator's E-Safeguarding files.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported E-Safety incidents
- Monitoring of network activity – policy central??

- Evaluation of children's work
- Discussions at children's groups i.e. school council
- Monitoring planning and evidence of work

Roles and responsibilities:

Governors:

Governors are responsible for the approval of the E-Safeguarding policy and for the reviewing the effectiveness of the policy. This will be carried out at E-Safeguarding Committee meetings. The Governor responsible for E-Safeguarding is ??

The role of the Governor will include:

- Attending E-Safeguarding committee meetings
- Monitoring of the E-Safety logs
- Reporting/Updating the Governing body at Governors meetings

Head Teacher and Leadership Team:

The role of the Head and Leadership team includes:

- The Head Teacher is responsible for ensuring the safety (including E-Safety) of members of the school community
- The Head/Leadership team are responsible for ensuring that other staff receive suitable CPD to enable them to carry out their duties and to train other colleagues as appropriate.
- The Head/SLT are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. This is detailed within the child protection policy.

E-Safety Coordinator (Deputy Head):

The role of the E-Safety Coordinator includes:

- The day to day responsibility for E-Safeguarding issues and has a leading role in establishing and reviewing the school's E-Safeguarding policy.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place
- Receiving and reporting reports of E-Safety incidents and recording all incidents in the E-Safety log.

- Ensuring that all incidents are dealt with according to the school behaviour policy and that the Class Teacher, Parents and other parties are informed where appropriate.
- Coordinating the E-Safety Committee meetings.
- Monitoring and reviewing the E-Safety teaching and learning taking place across the school.
- Monitoring and reviewing the weekly Smoothwall filtering reports via Bradford LA that are received via e-mail on a termly basis.

Technician

The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack.
- That he keeps up to date with E-Safety technical information and updates the E-Safety Coordinator as relevant.
- That monitoring software and antivirus software is implemented and updated.

Teaching and support staff

Teaching and support staff will:

- Keep an up to date awareness of E-safety matters and the current E-Safety policy through staff meetings and training sessions
- Read, understand and sign the school Acceptable Use Policy (see appendix)
- Inform the Head Teacher of E-Safety incidnets which will then be recorded in the E-Safety log
- Report any suspicious misuse or problem to the E-Safety Coordinator for investigation
- Ensure that all digital communications with pupils should be professional and only carried out on official school systems
- Ensure that E-Safety issues are embedded in all aspects of the curriculum
- Ensure that E-Safety lessons are planned and taught every half term and that the lessons are age appropriate/reflect the needs of the age group (see Computing policy in appendix)
- Ensure that they are aware of the 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 regards to these devices.

Designated Safeguarding Lead for child protection

The Designated Safe-guarding Leads are trained in E-safety issues and are aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate contact with adults/strangers

- Potential incidents of grooming
- Cyber-bullying

Pupils

Pupils are responsible for using the school ICT systems and equipment in accordance with the Pupil Acceptable Use Policy. They are briefed annually on the content of these policies which they are then asked to sign. Signature forms require parental signatures as well. Forms are collected and stored in the school office.

Pupils are encouraged through E-Safety/PSHE lessons to share any E-Safety concerns with a trusted adult.

Parents/Carers

The school will take every opportunity to help parents/carers to understand E-Safety issues. We will raise awareness of the key issues in the following ways:

- Parent/Carer assembly on E-Safety
- Pupil Acceptable Use Policy are available on the school's website. Parents are asked to discuss these with their child.
- Information about E-Safety and parental resources are available on the school website
- Information is also shared via letters and newsletters

Pupil Education

The education of pupils in E-Safety is a crucial part of the school's E-Safety provision. Children need the help and support of the school to recognise and avoid E-Safety risks and to build their awareness of how to keep themselves safe. E-Safety education will be provided in the following ways:

- A planned E-Safety programme is delivered through ICT and PSHE in the form of the TIC Bradford scheme
- The Bradford ICT Scheme of work also highlights E-Safeguarding issues that arise in the context of ICT lessons
- Pupils are taught in all lessons to be aware of the content that they access on line and learn how to validate the accuracy of the information they find
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

- Copyright free images and audio sources are shared with the children and are included in the Bradford ICT Scheme of work
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children
- Pupils know that any events of Cyber-bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult

Internet provision

The school Internet is provided by BLN (Bradford Learning Network), which is in line with Internet Watch Foundation CAIC lists and other illegal content lists. There are clear monitoring and reporting systems in place to update lists and identify breaches.

Managing ICT systems and access

Access to ICT systems is managed by the Technician and ICT/E-Safety Coordinator. All children at the school receive logins and accounts for: school systems and e-mail. These accounts are managed through administrator privileges which are only known to the Technician and Coordinator. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6.

Adult accounts and passwords are also created in the same way. Adults are given accounts for school systems, e-mail and the school blog. Accounts are created and deleted for new starters and leavers when required.

Passwords

All users (staff and pupils) have the responsibility for the security of their user name and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the E-Safety Coordinator.

- Passwords for new users and replacement [passwords for existing users can be allocated by the E-Safety/ICT Coordinator.
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the E-Safeguarding policy.
- Pupils are made aware of the school's password rules through ICT/E-Safety lessons and through the Pupil Acceptable Use Policy.
- Old user names and accounts are deleted annually.

All pupils have their own individual log in and password for accessing the school's ICT systems, the school blog and school e-mail accounts with the exception of children in KS! Who have their own individual user names but all have the same password.

Personal Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All staff must ensure the:

- Safe keeping of personal data at all times to minimise the risk of its loss or use
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Ensure that memory sticks where used are password protected
- Ensure that information is saved on secure drives which can only be accessed by password

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images.
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment; personal equipment should not be used for these purposes. All classes now have a class ipad for this purpose.
- Parental permission to use photographs on the school website, blog and in the press must be given.
- Photographs will be published without names on the blog, website and in the press. In incidences where names are required (some newspapers) parental permission will be sought.
- Teaching staff are responsible for storing photographs and images safely and securely.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should immediately complete a cause for concern form in line with our Child protection procedures and hand to a Designated Safe-guarding Lead. It is important that the device is not shut down as evidence could be erased but that it is removed to secure site. All matters should be reported immediately to the Head/E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Whilst it is impossible to record possible sanctions for every eventuality a list of types of misuse and sanctions are included in the appendix to this policy.

Cyber bullying

Cyber bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

Pupils are taught about cyber bullying through E-Safety and PSHE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and, where possible, screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. The school may report serious cyber bullying incidents to the Police.

Social Media

St Walburga's School uses Social Media in the following ways:

- A Text to Parents system which is managed by the school office. This is used as a reminder service for parents.
- As part of our school website pupils have a blog they can contribute to. All comments and posts are moderated by teachers before they are published. Pupils know that they must not share personal information on the blog or use it to communicate with people they do not know in real life.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. The *school's* use of social media for professional purposes will be checked regularly by the E-Safety committee to ensure compliance with this policy.

Mobile devices

Staff

Staff must not use mobile phones in lessons. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. Except in urgent or exceptional situations, whereby the owner will seek permission from the Head teacher, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. In accordance with the Acceptable Use Policy, staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

Pupils

School does not allow children to bring mobile phones into class. All mobile phones are stored in the school office. As part of the E-safety scheme of work, pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School mobile devices

The school has a variety of mobile devices including iPads. All of the statements included in the Acceptable Use Policy apply to these mobile devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

We have detailed Acceptable Use Policies for staff. This is included in the appendix of this policy.

Development and Review of this policy

The implementation of this policy will be monitored by the E-Safeguarding Committee.

Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to E-Safety of incidents that have taken place.

Should serious E-Safety incidents take place, the following external persons/agencies should be informed: Jenny Sadowski, Safeguarding Officer, Bradford Council, Bradford Learning Network.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

Policy Date: Feb 2015 Review Date: Feb 2016

This policy has been approved and adopted by the Governing Body.

Signed .... (Chair of Governors) Date...........................