St Mary's Bryanston Square CE Primary School

Draft Online Safety Policy 2015

"Excellence with compassion"

Our Vision

To provide an excellent learning environment, which promotes achievement in every area, and nurtures the social, emotional and spiritual well-being of the whole school community.

1. PURPOSE

This policy statement relates to online safety for all pupils from 3-11yrs within at St Mary's Bryanston Square CE Primary School.

2. AIMS AND OBJECTIVES

The aims for this policy are to ensure the safety of all children and adults at St Mary's Bryanston Square CE Primary School.

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Mary's Bryanston Square CE Primary School with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of St Mary's Bryanston Square CE Primary School.
- 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 online bullying 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.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. The internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; ICT can offer new weapons for bullies, who may torment their victims via websites, text messages, emails or social media; children and young people can also be exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied within the school.

This policy document is drawn up to safeguard everyone at the school – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

3. ONLINE SAFTEY PRACTICE IN SCHOOL

Online safety in school will focus on:

- providing a safe environment for children with regards to their use of technology in school
- providing a safe environment for children with regards to the school and staff usage of technology in school
- educating children in how to use technology, particularly the internet, safely and providing guidance for children, parents, staff and other stakeholders in how to protect the well-being of all children with regards to technology

3.1 Providing a safe ICT learning environment in school involves:

- ensuring that children only use approved websites, programmes and technology when they are in school
- reporting any inappropriate content not filtered by the LGFL firewall
- not allowing mobile phone use during school time
- teaching children to use all technology safely (see 3.3. below)
- ensuring that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law

3.2 Providing an environment which is kept safe by staff and the school involves:

- Planning Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Following Rising Stars Switched on to Computing which contains built in online safety references which all teachers must make sure they teach and make references to in their planning.
- Modelling safe and responsible behaviour in their own use of technology during lessons.
- ensuring that information about and photographs or videos of children are not shared without the permission of their parents
- ensuring that information about and photographs or videos of children are kept safe (i.e. not on the mobile phones of staff or other stakeholders and files on computers are password protected)
- ensuring that any information not appropriate for children held by staff or other stakeholders is password protected and kept private
- ensuring that the school website does not contain personal information for pupils or staff
- ensuring that pupils' full names are not used anywhere on the school website

3.3 Educating children and parents in a range of current technologies:

Pupil Online safety curriculum

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (e.g. http://www.msn.com, http://info.aol.co.uk/aim/) often using web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (e.g. www.myspace.com / www.facebook.com/ www.bebo.com / www.twitter.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms
- Gaming Sites (e.g. www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/)
- Mobile phones with camera and video functionality
- Phones/ iPods with internet access (e.g. iPhone, Blackberry)

Children are very aware and competent in using these technologies and need to be explicitly taught the need for safe usage, e.g. privacy settings, implicit dangers of internet 'stranger danger' and the role of technology in bullying. Pupils should be taught regularly what to do if they experience material that they find distasteful, uncomfortable or threatening. Pupils should know that in these situations they should tell an adult they trust about what they have found.

Both children and parents should be aware of the age limits on some websites, particularly social networking sites such as Facebook, and the way these websites can potentially be abused. We will also run a rolling programme of advice, guidance and training for parents to ensure that principles of online safe behaviour are made clear for school and home us, and that they know who to contact if they need support

4. ROLES AND RESPONSIBILITIES

Online safety is recognised as an essential aspect of strategic leadership in the school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.
The Headteacher ensures that the Policy is implemented and monitors compliance with the Policy. Responsibility for online safety lies with the Designated Person for Child Protection, Toni McSherry (Deputy Headteacher).

4.1 The role of the Headteacher is to:

- ensure the staff keep up to date with online safety issues and guidance through liaison with Local Authority and through regular safeguarding training.
- liaise with Joskos and LGfL to ensure filtering systems are operating adequately and that inappropriate websites are blocked.
- receive regular monitoring reports from the online safety leader
- monitor and support staff who carry out internal online safety procedures (e.g. network manager)

4.2 The role of the governors

- To ensure that the school follows all current online safety advice, nationally and locally, to keep the children and staff safe
- To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Community and Values Committee receiving regular information about online safety incidents and monitoring reports.
- To support the school in encouraging parents and the wider community to become engaged in online safety activities

4.3 The role of class teachers and support staff:

- To read, sign and adhere to the Acceptable Use Policy
- To promote and support safe behaviours in their classrooms and following school online safety procedures.
- Safe use of school network, equipment which contain pupil information and data (always using own logins and passwords)
-

All staff should be clear about:

- Safe and appropriate use of personal e-mail, internet and mobile phone use in school (<u>not</u> during teaching or meeting times)
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network (ensuring personal information is kept private and any public information is commensurate with professional roles)
- Their role in providing online-Safety education for pupils

5. SCHOOL WEBSITE

The school website is the responsibility of the Headteacher and can be updated only by staff given access with the Headteacher's permission. All content on the website should comply with this policy and provide a safe environment for children and their families to discover information about the school. Any content deemed to be inappropriate should be reported to the Headteacher and immediately removed from the site.

6. CURRICULUM

In line with the National Curriculum, 2014, teachers should ensure that online safety is taught throughout the curriculum. Pupils should be taught:

- To use technology safely and respectfully, keeping personal information private (including for example, full names, school address, email addresses, names of friends, clubs attended)
- To be able to identify where to go for help and support when they have concerns about content or contact on the internet of other online technologies
- To recognise acceptable/unacceptable behaviour
- About the role of CEOP (Child Exploitation and Online Protection)
- To consider how public information is when using private areas of websites
- To consider how personal information can be regarded when posting a photograph onto a website (e.g. location, house number, street name)

7. REPORTING E-SAFETY CONCERNS

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 procedures to follow and consequences to be employed in the case of inappropriate use of ICT.

If inappropriate content is accessed unintentionally, children must report this to their class teacher, who in turn should notify the Headteacher. Similarly, if staff access inappropriate content unintentionally, they should report this immediately the Headteacher.

Consequences for inappropriate use of new technologies may include:

- Worklife Support Team on 0845 873 5680 / 020 7700 8370 (www.worklifesupport.com).
- interview/counselling by member of SLT/ Headteacher (as appropriate)
- informing parents or carers (with permission from the Headteacher)removal of internet or computer access for a period [which could ultimately prevent access to files held on the system]
- referral to LA / Police

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. The CEOP (Child Exploitation and Online Protection Centre) can provide guidance for children and staff/ parents in how to report internet bullying or abuse.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

8 REVIEW AND MONITORING

- The school has a Designated Safeguarding person who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The Online Safety policy has been written by the school Safeguarding Leader 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. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

Toni McSherry

December 2015

To be reviewed: Autumn 2017

Appendix 1

Online Safety Rules for EY and KS1

Think then Click

These rules help us to stay safe when using computers or the internet:

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do
- We can search the internet with an adult
- We only send polite messages on the internet when an adult is with us
- We tell an adult if I see something that upsets me when I'm using the internet

Online Safety Rules for KS2

Think then Click

- We ask permission before using the internet
- We only use websites that an adult has chosen
- We immediately close a webpage that we are not sure about and tell an adult about it
- We tell an adult if we something that makes us feel uncomfortable
- We send polite and friendly emails when an adult has given us permission
- We never give out any personal information on the internet
- We keep passwords private
- We never arrange to meet anyone we don't know

Appendix 2

Children's Contract to be signed by each child in Key Stage 2.

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own year group log in.
- I will not access other people's files.
- I will only use the computers for school work and homework.
- I will not bring any portable data storage into school without a teacher's permission.
- I will ask permission from a member of staff before using the Internet.
- I will not download program files from the Internet.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my home address or telephone number, or arrange to meet someone.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- To help protect other pupils and myself, I will tell a teacher if I see something inappropriate on a website.
- I know that my use of the computer, school network and other technologies may be monitored

Signed: _____ Class: _____ Date_____

Parent:
I agree that my child's work may be electronically published. I also agree that appropriate images and video that include my child may be published (*names of pupils will not be included when photographs are published)*.

I have read and understood the school online rules and give permission for my child to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Name of parent/carer: _____ Signed:_____ Date_____

Appendix 3

Websites offering additional advice and guidance:

BBC Chat Guide
http://www.bbc.co.uk/chatguide/
Becta
http://www.becta.org.uk/schools/esafety
Childline
http://www.childline.org.uk/
Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk
Grid Club and the Cyber Cafe
http://www.gridclub.com
Internet Watch Foundation
http://www.iwf.org.uk/
Internet Safety Zone
http://www.internetsafetyzone.com/
Kidsmart
http://www.kidsmart.org.uk/
NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209
NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog
Schools ICT Security Policy
http://www.eiskent.co.uk (broadband link)
Stop Text Bully
www.stoptextbully.com
Think U Know website
http://www.thinkuknow.co.uk/
Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/