MANCHESTER CHILDREN'S SERVICES
An I.C.T SAFEGUARDING POLICY FOR SCHOOLS AND SETTINGS

For

St Mary's C.E Primary School, Moss Side

1 INTRODUCTION

*This policy has been developed to ensure that all adults in **St Mary's C.E Primary School** are working together to safeguard and promote the welfare of children and young people and promote effective learning through information technology. As a 'Level 2' Rights Respecting School, we believe that information technology is an essential 21st century platform for delivering outstanding learning, business and communication. St Mary's recognises the importance of providing pupils, parents, staff and governors at St Mary's with an E-Learning policy that prevents distress and upset, prevents bullying and promotes outstanding learning and business through safe and secure systems, expectations and procedures. This policy ensures that the pupils of St Mary's have the following Children's Rights from the UNICEF Children's Rights Charter.*

Article 12: Your right to say what you think should happen and be listened to.

Article 13: *Your right to have information.*

Article 17: Your right to honest information from newspapers and television that you can understand.

Article 28: Your right to learn and to go to school.

Article 29: Your right to become the best that you can be.

Article 32: You should be protected from work that is dangerous.

Article 34:The government should protect children from sexual abuse

1.1 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.2 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.3 The Deputy Headteacher (Phil Trohear) or, in their absence, the authorised member of staff for e-safety (Sageguarding Lead, Julie Jackson) has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care. Both staff members will report immediately any safeguarding concerns and have regular dialogue with the Headteacher.

1.4 This policy complements and supports other relevant school and Local Authority policies.

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

1.6 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

2 ETHOS

2.1 It is the duty of the school to ensure that every child and young person in it's care is safe. The same 'staying safe' outcomes and principles outlined in the 'UNICEF Children's Rights Charter' apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and it's everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

3.1 The Headteacher will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff that have access to appropriate ICT training.

3.3 The Designated Senior Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and aware of the school's E-Learning/Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

4 TEACHING and LEARNING

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DCSF.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5 MANAGING INTERNET ACCESS

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people (this is also part of the policy on use of social media).

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via Mr Trohear.

5.4 The Smoothwall filtering software will monitor all internet use through the St Mary's internet and St Mary's wifi. Smoothwall will any identify inappropriate use and report this to the lead for I.C.T safeguarding.

5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

5.7 YouTube will be filtered through an adult log on filter process so no pupil can access the web-site. Staff will be advised that they must log off the computer if they are not in the room. All pupil accounts will have no access to YouTube, Facebook and Twitter.

5.8 All new staff must be given a copy of the ICT safeguarding policy and the Social Media Policy.

6 MANAGING E-MAIL

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Pupils and staff may only use approved school e-mail accounts for communicating through work (name@st-marys-mossside.manchester.sch.uk)

6.3 Pupils must inform a member of staff immediately if they receive an offensive e-mail or message through any form of internet software. This will be immediately reported to The ICT safeguarding lead.

6.4 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.5 There will be no access to external personal e-mail accounts for children unless it is for curriculum purposes.

6.6 The forwarding of chain letters is not permitted.

6.7 Incoming e-mail for staff should be monitored by staff and attachments should not be opened unless the author is known. Record and suspicious e-mails and report to Designated Senior Member for E-Learning.

7 MANAGING WEBSITE CONTENT

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Headteacher, Deputy Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused.

7.7 The names of pupils will not be used on the website, particularly in association with any photographs.

7.8 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8 SOCIAL MEDIA (Facebook, Twitter, Whatsapp e.t.c)

8.1 Please refer to the St Mary's Policy on use of Social Media.

9 MOBILE PHONES

9.1 No mobile phones for pupils will be permitted.

9.2 A school mobile will be accessible for staff to be used on trips, excursions and activities outside the school premises. The school mobile phone will be used by the staff to contact school.

9.3 The staff will not use mobile phones in the classrooms, school corridors when the pupils are present or learning unless permission is given by senior management in an emergency.

10 FILTERING

10.1 The school will work in partnership with parents/carers, the Local Authority, the DFE to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 Any material the school deems to be unsuitable or illegal will be identified by Smoothwall (St Mary's internet filter). A regular report will be generated produced identifying all types of internet activity.

10.3 Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.4 Filtering methods will be selected by the school in conjunction with the incumbent IT provider (MGL) and will be age and curriculum appropriate.

11 AUTHORISING INTERNET ACCESS

11.1 All staff must read the school's 'Policy of use of Social Media' before using any school ICT resources and any staff not directly employed by the school will be asked to read the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site.

11.2 I.C.T systems are accessible to all pupils / staff and visitors through individual and class logons.

11.3 The school will maintain a record of pupils whose parents/carers in the event of a specific request that their child be denied internet or e-mail access.

11.4 Parents/carers will be informed of the school's 'Acceptable Use' document and give permission for their child to access ICT resources.

11.5 Staff will supervise access to the internet from the school site for all pupils at all times.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 Staff may use photographic or video technology to capture to support school trips and these technologies will be used for appropriate curriculum activities.

12.2 Audio and video files may only be downloaded for appropriate educational purposes, adhering to copyright regulations.

12.3 Pupils must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.

12.4 Video conferencing and webcam use will be appropriately supervised for the pupil's age e.g. Third Space Learning.

13 ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Headteacher will ensure that the I.C.T Safeguarding Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for Internet access will be posted in all rooms where computers are used.

14.2 Responsible Internet use, covering both school and home use, will be included in computing lessons and through the rights respecting ethos.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

14.5 Discourage pupils from using social networking sites.

15 CONSULTING STAFF

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's conduct in the Policy of use of Social Media for ICT' and will be provided with a copy of the School Internet Policy and it's importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be for educational purposes, inappropriate internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.

16 MAINTIANING ICT SECURITY

16.1 Unapproved system utilities and executable files will not be allowed in pupils'work areas or attached to e-mails.

16.2 The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

17 DEALING WITH COMPLAINTS

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures. It is clearly identified on the school web-site the process for complaints around safeguarding at St Mary's.

17.2 The school's designated person for e-safety (Mr Trohear) will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.

17.3 Pupils and parents/cares will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.5 As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Disciplinary action
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system.
- Referral to the police.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's I.C.T Safeguarding Policy which may be accessed on the school website or the school office.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/cares without undue alarm.

18.3 Advice on appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers, on the web-site, suggestions for safe internet use at home will be available.

18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

19 COMMUNITY USE

19.1 School ICT resources may be increasingly used as part of the extended school agenda.

19.2 Adult users will sign the school's acceptable use policy.

19.3 Parents/carers of children and young people under 16 years of age will be required to sign the acceptable use policy on behalf of their child, as part of the agreed community use.