

E-safety Policy for Scalford Church of England School

Including use of cameras and mobile devices.



Headteacher:

M. A. Wang

02.02.15

Signed (Chair of Governors)

Date.....

Review date: February 2015
To be reviewed on or before February 2017

1. Introduction
2. Scope of Policy
3. Infrastructure and Technology
 - 3.1 Partnership working
4. Policies and Procedures
 - 4.1 Use of new technologies
 - 4.2 Use of cameras and mobile devices for photographs / images
 - 4.3 Reporting abuse
5. Education and Training
6. Standards and Inspection
 - 6.1 Monitoring
 - 6.2 Sanctions
7. Working in partnership with Parents and Carers
8. Appendices of the E-safety Policy

Consider which of the following policies are relevant

[Appendix A: Authorised Acceptable Use Policy – Staff, Volunteers and Governors

Appendix B: Acceptable Use Policy - Pupils

Appendix C: Equipment – Onsite and Offsite

Appendix D: Printers and Consumables

Appendix E: Data Security and retention

- *Back up procedures*
- *Disaster recovery*
- *Contingency planning*

Appendix F: Internet and email

- *External services*
- *Web mail*
- *Blogs and blogging*
- *Podcasting*

Appendix G: Privacy and data protection

Appendix H: Management and information systems

- *Joining of Administration and Curriculum Networks*

Appendix H: Support services

Appendix I: School website

Appendix I: List of authorised persons]

Scalford Primary School E-safety Policy

1. Introduction

- 1.1 Scalford Church of England School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.
- 1.2 As part of our commitment to learning and achievement we at Scalford School want to ensure that new technologies are used to:
- Raise standards.
 - Develop the curriculum and make learning exciting and purposeful.
 - Enable pupils to learn in a way that ensures their safety and security.
 - Enhance and enrich their lives and understanding.
- 1.3 We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give disabled pupils increased access to the curriculum to enhance their learning.
- 1.4 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.
- 1.5 The nominated senior person for the implementation of the School's e-Safety policy is the Head teacher.

2. Scope of Policy

- 2.1 The policy applies to:
- all pupils;
 - all teaching and support staff (including peripatetic), school governors and volunteers;
 - all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.
- 2.2 Scalford School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;
- close supervision of pupils when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Scalford School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the PrimaryWorld / EXA who provide a managed (not 'locked down') network system. We fully support and will continue to work with embc to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures .

3.1.3 We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

4.1.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 Scafold School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:¹ These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users are not allowed to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

4.1.5 In addition, users are not allowed to:

- Use the EXA / primary World or an equivalent broadband provider's facilities for running a private business;

¹ For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Enter into any personal transaction that involves embc or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of embc or member Local Authorities or adversely impact on the image of embc;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of embc, or to embc itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via embc
- Undertake activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via the embc network and the effort of staff involved in support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the embc network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after embc has requested that use cease because it is causing disruption to the correct functioning of embc;
 - other misuse of the embc network, such as introduction of viruses.
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.1.6 Where EXA (provider of Internet connectivity and associated services to schools) and/or PrimaryWorld become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Use of Mobile Phones, mobile devices for photography.

- 4.2.1 Children have their photographs taken to provide evidence of their academic achievements for developmental records particularly in the Early Years Foundation Stage. However, it is vital that any photographs or images are stored correctly to avoid any illegal or unacceptable use of these images. Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own recordings.
- 4.2.2 Under the Data Protection Act 1998, the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on school laptops / ipads, which are password protected until the school ceases to operate. Should this occur then the photographs will be shredded or deleted from any school device. Images should be downloaded as soon as is possible.
- 4.2.3 Photographs / images of pupils should not leave the premises unless on a device which is password protected / encrypted. If the equipment is available, staff removing images off devices should do so on site. If the equipment is not available in school, the Designated Senior Person should be notified. Images should not be carried on transferrable devices such as memory sticks unless encrypted. Staff may be required to complete a mobile device form if transporting sensitive material off of the school site.
- 4.2.4 Photographs should be printed in school and then removed from the cameras memory.
- 4.2.5 Photographs may be taken during indoor, outdoor activities and displayed on the website, promotional material e.g. prospectus and in children's work. On the website, children's names should not be displayed under photographs. Parental consent should be sought for media permission e.g. website, prospectus and newspapers.
- 4.2.6 Events such as Sports Day, Trips, Fundraising Events, Performances, may be recorded by video and photographs by staff and parents / carers, but this should be in view of others attending.
- 4.2.7 Many mobile phones have cameras built in so staff mobile phones should be turned off, must not be carried around in pockets and should be left with personal belongings. Visitors / staff may only use mobile phones in the school in non teaching areas and not during teaching times.
- 4.2.8 Cameras and mobile phones are prohibited in the toilets. If a photograph is required for a specific purpose e.g. washing hands linked to PSHE, then the member of staff must inform the designated senior person and should not take a photograph on their own.

- 4.2.9 In cases of a personal emergency all personal calls should be directed through the school office.
- 4.2.10 Staff are asked not to make personal calls during the working day. However, in urgent cases, or if deemed acceptable and necessary, permission can be sought from a senior member of staff. We acknowledge that use of mobile phones may not be possible due to the network coverage. Any requested for personal calls, incoming or outgoing, should be made to the senior member of staff on site, to agree use of the school phone, where deemed reasonable.
- 4.2.11 The school mobile phone should be used for off-site activities and should be used as the source of contact, should a mobile phone need to be used.
- 4.2.12 All devices which contain images of children should be locked away until required. Base staff are responsible for the location of their class cameras / ipads and individual staff for their ipads.
- 4.2.13 It is the responsibility of all members of staff to be vigilant and report any concerns to the line Managers.
- 4.2.14 Any non-compliance will be taken seriously, logged and investigated appropriately in line with our disciplinary policy.

4.3 Reporting Abuse

- 4.3.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately.
- 4.3.2 The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB² Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures³ assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

- 5.1 Scalford School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

² Chapter 9 of the LSCB Procedures

³ Chapters 5, 9, 12 and 13 of the LSCB Procedures

5.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

5.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.
- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures .

6. Standards and Inspection

Scalford School recognises the need regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use .

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, Scalford School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

6.1.3 We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Sanctions

6.2.1 We will support pupils and staff as necessary in the event of a policy breach.

6.2.2 Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

- *Child / Young Person*
 - The child/young person will be disciplined according to the behaviour policy of the school.
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- *Adult (Staff and Volunteers)*
 - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to the Designated Senior Person (Head teacher) and EXA / Primary World so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 Related aspects of the school's E-safety policy include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention.

Legal framework

Primary legislation

- Children Act (1989 s47)
- Protection of Children Act (1999)
- Data Protection Act (1998)
- The Children Act (Every Child Matters) (2004)
- Safeguarding Vulnerable Groups Act (2006)

Secondary legislation

- Sexual Offences Act (2003)
- Criminal Justice and Court Services Act (2000)
- Equalities Act (2006)
- Data Protection Act (1998) Non Statutory Guidance