St James The Less Primary School

Primary Online Safety Framework Document

Reviewed September 2019

Please use the following document to help you interpret this policy for our school.

- The Lancashire eSafety Guidance Document

The Lancashire eSafety Guidance Document offers support and prompts to enable you to consider the appropriate responses to eSafety in your school and is intended to be used alongside this policy.

This completed eSafety Policy forms part of the Lancashire eSafety Charter.
For further information about the Lancashire eSafety Charter please see http://www.lancsngfl.ac.uk/esafety

Terms of reference
eSafety – used throughout this document relates to all electronic Safety such as Online Safety /Web Safety / Electronic Device Safety

Developing and Reviewing this Policy

This eSafety Policy has been approved by Governors and will be monitored and reviewed as listed below:

The implementation of this policy will be monitored by E Safety Champions – Governor – Mr K Egan and Teacher Miss Dickinson

This policy will be reviewed as appropriate by annual review

Contents

Developing and Reviewing this Policy 2

Contents 3

1. Introduction 4

2. Your school's vision for eSafety 4

3. The role of the school's eSafety Champion 4

4. Policies and practices 5

4.1 Security and data management 5

4.2 Use of mobile devices 6

4.3 Use of digital media 6

4.4 Communication technologies 7

4.5 Acceptable Use Policy (AUP) 9

4.6 Dealing with incidents 9

5. Infrastructure and technology 9

6. Education and Training 10

6.1eSafety across the curriculum 10

6.2eSafety – Raising staff awareness 10

6.3eSafety – Raising parents/carers awareness 10

6.4eSafety – Raising Governors' awareness 10

7 Standards and inspection 10

St James the Less RC Primary School

eSafety Policy

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact. Furthermore it will help ensure the safety for all adults who support children in their learning.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. St James the Less RC Primary School vision for Online Safety

At St James the Less RC Primary school we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology, is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our eSafety policy and arrived at in joint consultation during staff meetings. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view eSafety education as a key life skill. At St James the Less we aim to equip children with the skills required to make appropriate life choices using the tools of the 21st Century learner and enjoy the benefits of such technologies as a rich, rewarding and safe experience.

Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils, parents, and all involved in our school community and is updated in light of the introduction of new technologies or incidents.

3. eSafety Champion

The role of the eSafety Champion is covered by the Computing Coordinators – Infrastructure and Curriculum. Ultimately the champion for eSafety is the headteacher who ensures this is addressed as part of the school Safeguarding agenda item in staff meetings.

4. Policies and practices

This eSafety policy should be read in conjunction with all school policies and documents:

4.1 Security and data management

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

All staff are aware of what constitutes data i.e. Photos, records, assessment data, personal details

This list goes beyond pupils and staff and can relate to procedures in school or particular circumstances that should not be made publicly available i.e. School security / Processes for School closure etc

However, staff are reminded that all pupil data should be kept in the following locations

- Photographs – all photographs of children can only be taken by school issued cameras and downloaded to the school server in a 'Staff Only' location (there are two locations for this)
- Photographs cannot be taken on staff mobile phones and cannot be taken home
- Visiting parents for assemblies and productions are informed of the appropriateness of taking photographs at specific times. This is always done in consultation with parents and specific guidance is offered
- Files about children (such as Assessment Trackers / IEPs) are only stored internally on the same server. If teachers need to transport files via pendrives they should ensure that all sensitive data is removed or the pendrive is encrypted in case such is lost
- Staff logon using a secure password that they alone know. Pupils do not know the teacher login details. Login details (passwords) are not shared with colleagues. Only one Global login is supplied for Supply teachers (staff can no longer use Staff01)
- Pupil Logon : All children have unique login details for some programs and Years 3 to Year 6 have personal login to access their files
- All persons using the school network or school devices away from school (i.e. laptops) accept that such property and all the data content belongs to the school. The school monitors and has the right to look at any data which may indicate the use of that technology if it has been used on school systems i.e. Tracking cookies, looking at history.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the school staff handbook has an Appendix dedicated to the use of ICT in schools which sets out appropriate use of mobile technologies

Additional info:

Laptops and IPads are a mobile technology that teachers may be issued with by St James the Less. Any technologies issued by the school are bound by the same school policies and the files contained on them are restricted in the same way. School issued technology is solely intended for school business and prior permission must be sought from the Headteacher or designate for any personal use of school technologies

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- All staff and pupils should respect copyright and understand what constitutes infringement
- Terms and Conditions (T&Cs) for all software must be read before acceptance. Staff are reminded that there is a specific ordering process with specific members of staff who have authority to place orders. This must be considered carefully before downloading and agree to the Terms and Conditions of, often, Free Software.
- Some T&C's have financial implications and some T&C's have age restrictions as part of US law (often age 13 and above). Any deviation from age recommendation must be documented and authority sought from the headteacher as to why such deviation is appropriate. This would include DVD's, sound files, software and any other digital media not mentioned in this policy
- Parents are asked to sign a document each year for authority to use their child(ren) in a range of media. Children whose parents do not wish to have their children part of any publicity are made known to all staff. A list is available in every classroom and both offices.

4.4 Communication technologies

All digital communications should be professional in tone and content.

Email:

- Any email containing school related information should only be contained in school assigned email addresses not personal ones
- Email is not always secure and sensitive data should not be sent using unencrypted email
- Email encryption web sites are available and specific sensitive documents should be sent using the LEA secure email service. This is particularly important for SEN details, CAF etc. Lancashire LEA host their own email encryption service which is free to all teachers

TEXT:

Our school uses text to parents and any member of staff should ask the office staff to send out a message. Other members of staff are entitled to use this facility if they have received training

Social Networks:

Many adults and pupils regularly use Social Network sites, e.g. Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute. Refer to Staff Handbook for additional information.

Some general rules to adopt

- Members of staff should NEVER be 'friends' of children in school. This would be considered a serious breach of professional duty
- Members of staff should not be 'friends' of parents. However, there may be exceptions to this rule such as staff members whose children are in school and therefore a social circle exists out of school. Where such social circles exist all staff are reminded of the school Confidentiality Policy which prohibits particular conversation about school. No conversation should ever bring the school or themselves into disrepute or reveal anything about a pupil, staff member or school system. Staff are further reminded of the Whistle Blowing Policy that encourages all staff to make any such breaches clear to the headteacher
- All 'postings' should be considered to reflect the member of staff as a role-model to our pupils

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

Adults:

- Staff : Mobile phones are not allowed to be used in class or in any situation, especially if that adult has responsibilities for that class
- Authority to use a mobile phone in class must come from the headteacher or designate
- The use of the camera facility on mobile phones is forbidden

See staff handbook for additional information on Mobile phones

Children:

- The bringing of mobile phones into school is to be discouraged. However, some parents expect their child to have a phone for the independent journey home; these children should hand phones into the office and collect at the end of the day
- Children are expected to keep their phones in their pockets/bags on the journey home. This is to protect them from opportunist thieves and to ensure they are not distracted and therefore endangered (e.g. crossing roads)

See staff handbook for additional information on Mobile phones

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- In our school we do not permit the use of any Messaging service that the school does not have total control over.

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- Principles of VLE (Moodle) are the same as the rest of using technologies. Children are taught good etiquette when using VLE Platforms and encouraged to adopt this into their ICT use.
- Children should follow their teacher's direction in using the VLE appropriately
- Staff training for VLE alongside E-Safety is identified. No members of staff use VLE without suitable training and understanding of the school policies

Web sites and other online publications

- *School website is maintained by designated staff who are adequately trained to ensure all material uploaded is appropriate*

4.5 Acceptable Use Policy (AUP)

The rapid change and expansion of new technologies require a flexible, developmental and safe response to their use. With this in mind every effort will be made at St James the Less to allow staff to discuss freely how children should use new technologies appropriately. A regular slot is dedicated in every staff meeting to ensure acceptable use is maintained. The scope of acceptable use will likely change on a regular basis and our school has decided to build into each staff meeting a slot to raise these issues.

Sample AUPs may be appropriate for particular circumstances and can be found in the appendices of "eSafety Guidance Document – Primary eSafety from Lancashire County Council

4.6 Dealing with incidents

Staff are made aware of what constitutes 'illegal materials' and to report immediately to the headteacher or designate. If illegal material is found on screen to turn off the monitor and refer to www.iwf.org.uk and the POLICE. They must not show to other members of staff or any other person as this constitutes an offence.

Staff deviation from Policy will be dealt with as with any deviation from school policy

In the case of a child: any deviation from following teachers' specific instructions will be a direct contravention of the school Behaviour Policy which is supported by the Behaviour Consequence Chart. For instance- CyberBullying would be treated as Bullying and would fall into Level 3 Behaviour Consequence and would involve parents being informed. Children are taught what constitutes acceptable use of technologies and are encouraged to educate their peers so that all may use the technologies safely.

Training materials are used to appropriately educate teachers, children and parents

5. Infrastructure and technology

Pupil Access:

Children in KS1 have a generic login. Children in KS2 have their own unique login.

Passwords:

Nominated staff can change all passwords. Pupils should have own. All persons who use the school system are taught about password strengths

Software/hardware:

Auditing is carried out by the Headteacher and School Business Officer

Site Licenses are controlled by Technical Support which is provided externally. No applications are ever installed unless Tech Support is sure that the school is correctly licensed

Managing the network and technical support:

Detailed management of school wireless, network, server, client stations is controlled by Technical Support, further directed by nominated persons

Devolved Filtering : The headteacher accepts responsibility for Internet filtering. Normally all filtering is carried out by our ISP who recognise the need for school filtering

6. Education and Training

Education and training are essential components of effective eSafety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. eSafety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote eSafety.

Online safety

Appropriate filters and monitoring systems are in place to protect children against potentially harmful and inappropriate material online. These are supporting tools and not a solution therefore should be implemented to support and complement effective classroom practice. Children will be taught critical thinking skills when managing internet access which are appropriate to their age and ability.

6.1eSafety across the curriculum

E Safety week and part of teaching of ICT skills – Progression documents refer explicitly to E-Safety

6.2eSafety – Raising staff awareness

Training and Policy Review – Staff Agenda Item each week to discuss issues as they arise

6.3eSafety – Raising parents/carers awareness

Documentation sent home to parents through Splash News / Newsletter / Flyers. Additional information sent in letters as the need arises or at the start of the year when permissions are obtained . Further information is made available on the school website which reflects up to date changes to 21st Century technologies

6.4eSafety – Raising Governors' awareness

Governors are responsible for agreeing E Safety policy. Any incidents are communicated to governors as and when appropriate.

7 Standards and inspection

Monitoring of the policy will be done by the Headteacher and reported back to the Curriculum Committee of the governors.

ADDITIONAL INFORMATION

Note: This document should be used alongside the eSafety Guidance Document from Lancashire County Council which provides further examples