Packington Church of England Primary School

Online Safety Policy

But Jesus called them to him, 'Let the children come to me, and do not hinder them, for to such belongs the kingdom of God' (Luke 18:16)

Policy reviewed: Oct 2017
Date of next review: Oct 2019
Headteacher: Mrs C Price
Chair of Governors:

Online safety Policy

Contents:

Online-safety Policy
1. Introduction

When children leave us we want them to be compassionate, self-confident with a love of life and learning.'

The Bible verse that sets this vision in context is John 10:10 "*I have come that they may have life, and have it to the full."* ***For it is the flourishing in the grace of God that will enable our children to be wise, hopeful, live well together with dignity and respect in God's world.***

It is a vision that is inclusive to all as we are reminded in the words of Luke 18:16:
"But Jesus called them to him, saying, "Let the children come to me, and do not hinder them, for to such belongs the kingdom of God."
For we are all equal in the eyes of God.

1.1 Packington Church of England Primary 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 Packington Church of England Primary 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 Online Safety policy is Head Teacher Mrs Carol Price

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 Packington Church of England Primary 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 online 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 Packington Church of England Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership with others. We use online resources such as CEOP to support policy making and teaching. Year 6 visit the Warning Zone and learn about online safety. Our internet and broadband connection is overseen by our technician though ICT Independent Consulting limited who are highly experienced in schools technology and ensuring we have the correct protection in place.

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 online 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 online 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 online 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 Packington Church of England Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below: These expectations are also applicable to any voluntary, statutory and

community organisations that make use of the school's ICT facilities and digital technologies. All staff are expected to sign our acceptable use policy.

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 e.g. Youtube may be beneficial for educational use. In such circumstances, these can only be accessed by staff login procedures.

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 broadband provider's facilities for running a private business;
 Enter into any personal transaction that involves any member Local Authorities in any way;
 Visit sites that might be defamatory or incur liability on the part of the school or member Local Authorities;
 Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties;
 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
 Undertake activities with any of the following characteristics:

- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- other misuse of the 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.

4.2 Reporting Abuse

4.2.1 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 or may become aware of something on social media sites that is threatening or abusive. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident immediately. If the pupil visits a website they feel is inappropriate they are taught to click on 'Hector the Dolphin' which will hide the site until a teacher is notified. If the site is judged to be inappropriate the computing coordinator will be informed, it will be recorded and the technician will be informed to block the site.

4.2.2 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.

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

5. Education and Training

5.1 Packington Church of England Primary School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

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 online 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. We have a rolling two year programme taught through both computing and PSHE. We support Safer Internet Day each year and also year 6 pupils complete an online safety audit for Simon Genders of Leicestershire County Council safeguarding and we are able to anylase the results for any concerns. Year 6 also have a half day visit to the online safety section of Warning Zone.

- 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 online safety policies and procedures through our school website.

6. Standards and Inspection

Packington Church of England Primary School recognises the need to 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, Packington Church of England Primary 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. 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 behaviour 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.

If inappropriate material is accessed, users are required to immediately report this to the DSL 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. Our annual acceptable use policy is sent home at the start of the year for parents to share with children.

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.

7.3 Parents complete a form to give the school permission to use children's images on media such as twitter, blogs or our website.

8**. Appendices of the Online-safety Policy**

8.1 Related aspects of the school's online-safety policy include acceptable use policies for both staff and pupils. There are also links or references in this policy to our behaviour policy, our anti-bullying policy and our complaints policy.

List of authorised persons
The Designated Senior Lead (DSL) for safeguarding is the Headteacher – Mrs C Price This role incorporates reviewing and monitoring the policy for Online-safety.

The Deputy DSL is Mrs F Rogers

The DSL for the Governing Body is the Chair of Governors – Mrs C Harris-Marsh and Mrs C Hammond.

The office administrator (Katherine Pilbro / Natalie Marriott) is responsible for collecting data information sheets and for processing permission slips from parents for use of the internet and computer technologies in school.

The ICT Leader is Mr Emery. In his role as Computing leader he monitors teaching and learning of computing in school.

The ICT technician in school is procured personnel from ICT Independent Consulting Limited and has permission to set up passwords and usernames for children in school.

All teaching staff are responsible for ensuring online safety is a taught part of the curriculum for computing and also within elements of PSHE.

All teaching and support staff are responsible for ensuring children use their usernames and passwords sensibly.