# St Peter's C.E. Primary School

# E-safety safety Policy

**Reviewed September 2020**

**Our Christian Vision**

**As a Christian family at St Peter's School, we create a unique place of learning, nurturing the gifts that God in His awesomeness has given us. We encourage every child and prepare them for life's journey, inspiring them to fulfil their potential, their dreams and their aspirations.**

**Sowing the seeds of tomorrow.**

**(Matthew 13:1-23)**

**Intent**

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote children's achievement. However, the use of these new technologies can put them at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Un-authorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

**1. Development and Monitoring**

| **Role** | **Named person** |
|---|---|
| Computing Subject Leader/E-safety Leader | Kathy Williams |
| Computing Support | Tahira Khan |
| Designated Safeguarding Lead | Vicky Weddle |
| Data Protection Officer | Joyce Kirkham |

This e-safety policy has been developed by the Computing Subject Leader and the Designated Safeguarding Lead in conjunction with the School Leadership team.

As part of this policy, records will be maintained of E-Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures.

This policy will be reviewed annually.

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs

This policy applies to all members of the school community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other on-line e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

**3. Roles and Responsibilities**

<u>Governors</u>

- Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

<u>Headteacher/Senior Leaders</u>

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though day to day responsibilities. In the absence of the Headteacher, responsibility will be delegated to the Computing Co-ordinator/Designated Safeguarding Lead.
- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any new recommendations regarding further improvement.
- The Headteacher/Senior Leaders are responsible for ensuring that the Computing Subject Lead/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles.

- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Managing Allegations against a member of staff policy/guidance).

Computing Co-ordinator and Designated Safeguarding Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Reports to the School Leadership Team of serious breaches to the E-Safety Policies.
- Provides training and advice for staff.
- Liaises with the Local Authority
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Are trained in and share with staff an awareness and understanding of the e-safety issues and the potential for serious child protection issues that can arise from:

    - Sharing of personal data
    - Access to illegal/inappropriate materials
    - Inappropriate on-line contact with adults/strangers
    - Potential or actual incidents of grooming
    - Cyber-bullying
    - Sexting
    - Revenge pornography
    - Radicalisation (extreme views)
    - CSE

Teaching and Support Staff

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the E–Safety policy, school Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or problem to the Computing Subject Leader/Designated Safeguarding Lead for investigation/action/sanction.
- Digital communications with pupils and parents/carers (email/voice) should be on a professional level
- Children understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy.
- Children understand and follow E-Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies.
- In lessons where internet use is planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc.
- Should understand that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, the school website/ local e-safety campaigns/literature.

Parents and carers will be responsible for:
- Endorsing (by signature) the Student/Pupil Acceptable Use Agreement.
- Accessing the school website/on-line pupil records in accordance with the relevant school Acceptable Use Policy.
- Understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

**4. Education and Training**

Education of our children

E-Safety education will be provided in the following ways, as appropriate to the children's age and ability:

- A planned e-safety programme should be provided as part of Computing/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies inside and outside of school.
- Key e-safety messages should be reinforced as part of a planned programme of themed weeks and other appropriate pastoral activities.
- Children should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children are taught the importance of keeping information such as their password safe and secure.
- Rules for the use of ICT systems/internet will be made available for children to read.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- Children are taught how to keep safe though effective e-Safety practice as part of an integral element of the school Computing curriculum and within their ICT learning.
- Where children are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit.

Education of our Parents and Carers

Some parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, web site
- Parents evenings
- Reference to external e-Safety websites
- High profile events such as Internet Safety Day
- Family learning opportunities
-

Education and Training for our Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will monitored.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies.
- The Computing Subject Leader (or other nominated person) will provide advice/guidance/training to individuals as required.

**5. Technical – Infrastructure / equipment, filtering and monitoring**

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirements for Blackburn with Darwen Borough Council.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- Staff will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by BwD.
- Any incidents or activities regarding filtering will be handled in accordance with BwD.
- Remote management tools are used by the managed service provider to control workstations and view user activity.

- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest access to the school network will be authorised by the School Office Team through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.
- The school infrastructure and individual workstations are protected by up to date antivirus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy.

**6. Use of digital photographs and video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Written permission from parents or carers will be obtained before photographs of children together with their name are displayed on school displays, in newsletters and in their child's own and other children's learning journeys.
- Written permission from parents or carers will be obtained before photographs of children together with their name displayed alongside are published in leaflets, posters, documents, training materials or used by the press.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or social media. Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.

**7. Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school's Personal Data Policy.

**8. Communications**

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the e-Safety Coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and children or parents/carers must be professional in tone and content and be via official used systems.
- Whole class or group email addresses will be provided to all classes for educational use. Individual email addresses will be provided to children when needed and if deemed appropriate for their level of ability by their class teacher.
- Children should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their mobile phones, for their own use. When in school, under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

**9. Responding to incidents of misuse**

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by children, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

**10. Monitoring and review**

This policy will be reviewed annually, or earlier if necessary in line with national and/or local updates.

**The school e-safety Coordinator: Mrs Kathy Williams**

Signature: .....

**The designated member of the Governing Body responsible for e-safety: Mrs Laura Jenkinson**

Signature: .....

**Chair of governors: Andrew Robinson**

Signature: .....

# St Peter's CE Primary School
# Consent form for photographs and pupil work.

**Name of child** ..... **Date of birth** .....

**Name of parent** .....

St Peter's CE Primary School believes that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of pupils for internal display and displaying pupil work enables us to celebrate individual and group successes as a school community. We would also like to use photographs and videos of the school and its pupils to promote the good educational practice of the school. Children's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

By signing this form you are consenting to the use of images of your child being used in the following outlets under the terms outlined in section 7 of our online safety policy:

- All school publications
- On the school website
- In newspapers as allowed by the school
- In videos made by the school or in class for school projects

***Please read the questions below, circle your answers and then sign and date the bottom of the form. Please then return this form to the school office as soon as possible.***

1. Can we use your child's photograph in printed publications by St Peter's CE Primary School?
   **YES / NO**

2. Can we use your child's photograph on our website, school blogs, or the school's partnership websites either:

   - In a group or as a member of a whole school activity?
     **YES / NO**

   - Individually?
     **YES / NO**

3. Can we use your child's photo for publication in a newspaper?
   **YES / NO**

4. Can we photograph and video your child within school, and display these publicly within the school, as part of the curriculum and in class?
   **YES / NO**

5. Can we use videos of your children to share good practice with professionals from other schools?
   **YES / NO**

This consent form covers consent for the duration of your child's time at the school . Once your child leaves the school, photographs and videos may be archived within the school but will not be published without renewed consent. More information regarding the storage and protection of images can be found in the school **data protection policy**.

A full copy of the school's policy on online safety containing information on the safe use of photographs, videos, and the work of children in school can be found in the school office/on the school website.

Signed: ..... Date……