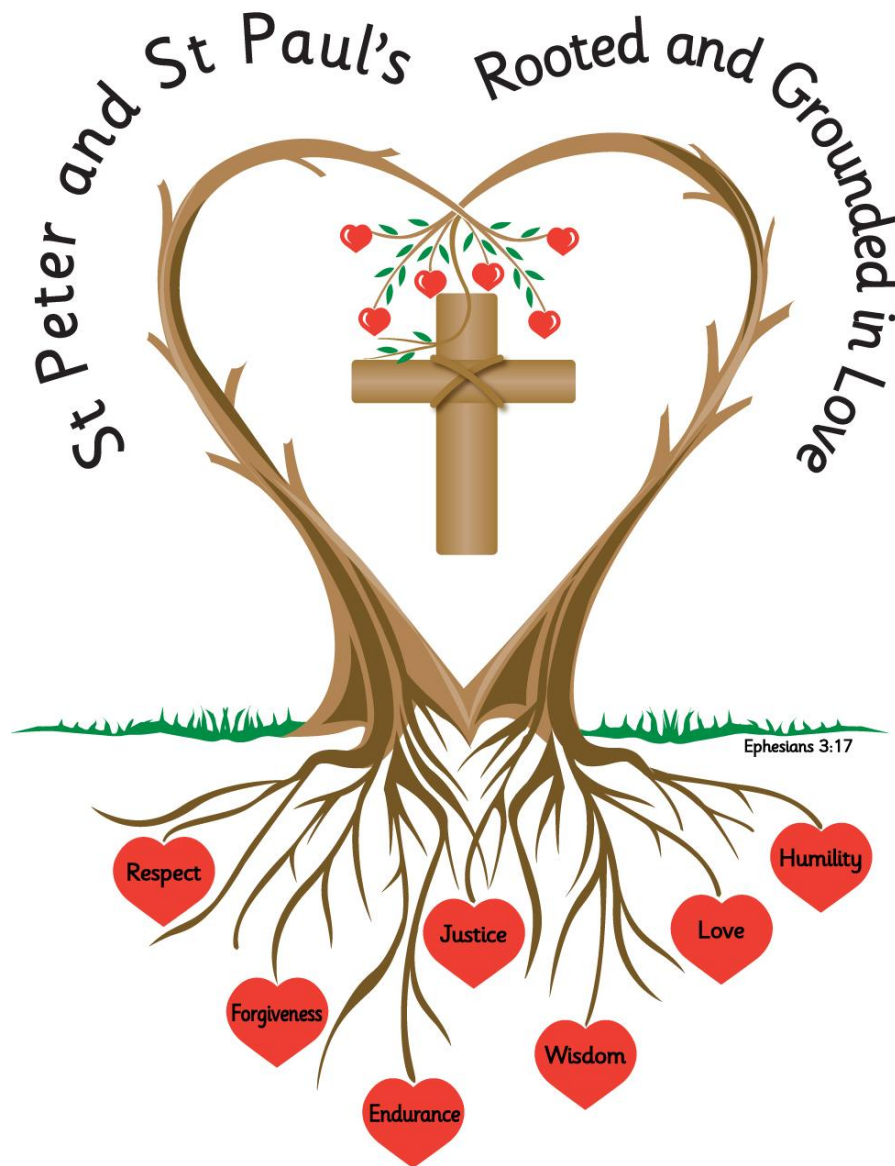


St Peter and St Paul's Church of England Primary School



Computing Policy

Being 'Rooted and Grounded in Love' (Ephesians 3:17) we strive to follow the Lord's command to love God above all things and each other as brothers and sisters, making God's Kingdom a reality in our school and throughout our community.

Online Safety

- 1. Introduction**
- 2. Effective Practice in Online Safety**
- 3. Teaching and Learning**
- 4. Managing Internet Access**
- 5. Policy Decisions**
- 6. Communications Policy**
- 7. Online Bullying**

Computing Policy

- 8. Introduction**
- 9. Vision**
- 10. Aims**
- 11. Curriculum Coverage and Progression**
- 12. Assessment**
- 13. Monitoring**
- 14. Foundation Stage**
- 15. Equal Opportunities and Inclusion**
- 16. Liaison and transfer between settings**
- 17. Home, school and community links**
- 18. Resources**
- 19. Roles and responsibilities**
- 20. Health, Safety and Security**
- 21. Review**

1. Introduction

St Peter and St Paul's CEP School fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of Internet and electronic communication technology such as mobile phones and wireless connectivity.

This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school online safety policy will operate in conjunction with others including policies for Good Behaviour, Anti-Bullying, Equal Opportunities and Internet Access Agreement with parents/carers.

2. Effective Practice in Online Safety

Online Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented Online Safety Policy;
- Secure, filtered broadband;
- A school network that is compliant with National Education Network standards and specifications.

2.1 Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for ICT, anti-bullying and child protection.

The school has appointed Online Safety Coordinators, these are the Computing Subject Leader, Designated Safeguarding Officers and the Headteacher.

3. Teaching and learning

3.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

3.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. The ICT technician through discussion with the Headteacher and Computing Subject Leader ensures this is kept up to date. The filter is provided under the CLEO network in conjunction with LCC.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.

3.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of crosschecking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content to the Online Safety Leader or, if the content is accessed at home, using the CEOP Report Abuse icon or Hector Protector.

4. Managing Internet Access

4.1 Information system security

- School Computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

4.2 E-mail

- Pupils in our school do not currently have personal e-mail accounts on the school system
- Email systems used through outside learning platforms such as Purple Mash seek adult approval before emails are sent to peers.
- In e-mail or other electronic communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mails from pupils to external bodies are controlled carefully by the class teacher or teacher supervising the activity.
- The forwarding of chain letters is not permitted.
- Threatening or offensive emails must be reported to an Online Safety Co-ordinator and recorded via CPOMs.

4.3 Published content and the school web site and Facebook

- When starting at the school parents are asked to provide permission for images of their children to be published on the school website and Facebook.
- Pupil personal contact information will not be published.
- All members of teaching staff have access to the school website and are responsible for ensuring information is accurate and up to date.
- The Computing Subject Leader, in conjunction with the Head teacher, will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or work of pupils is published on the school website or Facebook.
- Work published on the website will not be identified with an individual pupil.
- Pupil image file names will not refer to the pupil by name.
- Staff, parents/carers and pupils will be educated in the dangers of publishing images and videos of pupils or adults on Social Networking sites or websites without consent of the persons involved.
- It is not recommended that staff use their own digital media devices in school, however if this is a necessity, photographs/videos must be downloaded onto the school's secure network as soon as possible and files immediately deleted from own devices.

4.5 Social networking and personal publishing

- The school does not allow children to access social networking sites, but does educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.
- Applications such as Whataspp, Instagram and Facebook etc. should **NOT** be used due to age restrictions.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Networking sites.
- Adults do not communicate with pupils using any digital technology.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- No school issues, which could possibly breach school confidentiality or school policy, should be discussed on any blog or personal websites.

4.6 Mobile telephones

- School Office or staffroom telephones are used for all school related matters.
- Children are not permitted to use mobile phones in school. Those brought into school must be handed in at the office and parents must sign a form to say that they are needed for a specific reason e.g walking home alone.
- Staff personal mobile phones can be used on-site outside of working hours when children are not present. At other times mobile phones may only be used in the staffroom, office or carpark, where children are not present. At all other times, they are stored securely in lockers, with ringtones disabled.

4.7 Managing filtering

- School has a filtering system in place and reports are sent to the Computing Subject Leader.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Leader. It is vital that children and adults are aware of the necessary actions to take (minimise webpage, turn monitor off and tell a trusted adult immediately).
- Computing Leader and Head Teacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.8 Managing videoconferencing & webcam use

- Videoconferencing and webcam use will be appropriately and supervised by a member of teaching staff.

4.9 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access could bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Airdrop, Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will not be allowed throughout the school year. *There may be exceptions to this e.g Year 6 are able to take photographs of their classmates on the last day but only after parents have been notified first.*
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

4.10 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff who have remote access to school data must ensure the data remains secure by being aware of the dangers of using unsecured wireless access outside school.

5. Policy Decisions

5.1 Authorising Internet access

- All staff must read and sign the 'Appropriate Usage of ICT' document before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

5.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LCC can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.
- ALL staff are aware and have received training allowing them to report any issues/concerns/incidents via CPOMs.

5.3 Handling Online Safety complaints

- Any complaint about staff misuse must be referred to the Headteacher or Computing Lead.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Where appropriate, both pupils and parents will be informed of consequences for pupils misusing the Internet.

6. Communications Policy

6.1 Introducing the Online Safety Policy to pupils

- Online Safety rules will be posted in the ICT suite and in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in Online Safety will be developed, based on the materials from CEOP.
- Online Safety training will be embedded within the Computing scheme of work regularly throughout the academic year.

6.2 Staff and the Online Safety Policy

- All staff will have access to the School Online Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Staff are made aware of issues which affect their own personal safeguarding e.g. use of social networking sites.
- No staff member should accept an invitation from any pupil past (under 18 years of age) or present to 'add' them on to their friend contacts.
- Staff are expected to promote and model responsible use of ICT and digital resources.

6.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
- The school will maintain a list of Online Safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

7. Online Bullying

7.1 Defining Online Bullying

Online Bullying is a type of aggression defined by Childnet and adapted by our school, as the sending or posting of harmful or cruel text, images, videos or animated material using the internet or other digital communication devices.

7.2 What constitutes Online Bullying?

- 1. Text messages** – unwelcome texts that are threatening or cause discomfort.
- 2. Picture/video-clips via mobile phone cameras** – images sent to others to make the victim feel threatened or embarrassed.
- 3. Mobile phone calls** – silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- 4. Emails** – threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- 5. Chatroom bullying** – menacing or upsetting responses to children or young people when they are in a web-based chat room.
- 6. Instant messaging** – unpleasant messages sent as children conduct real-time conversations online.
- 7. Bullying via websites** – e.g. use of defamatory blogs (web logs), personal websites and online personal polling sites.
- 8. Bullying via online games** e.g Xbox

7.3 Education

- Pupils and parents know what pupils' responsibilities are in the use of information communications technology (ICT), and what sanctions will be imposed for misuse.
- The teaching staff have updated the anti-bullying policy as well as all other policies relating to behaviour, pastoral care, e-learning and existing acceptable use policies, to include references to the online bullying policy.
- Mobile phones can only be brought into school by pupils if there is a specific need e.g walking home alone and parents must sign a form. They must be switched off before entering school and left with the administration staff at the school office during the school day. Children attending after school clubs must store them in their bags in the same location as the ASC.
- Staff teach about bullying in PSHE, SEAL and Citizenship. The Subject Leader is working closely with other subject leaders to ensure that Online Bullying is included in all the related units.

7.4 Incidents of Online Bullying

- Incidents of Online Bullying will be recorded in conjunction with the schools anti-bullying policy. Evidence will be taken in conjunction with the Online Safety and Data Protection Policies.
- Staff and pupils are advised not to engage in Online Bullying if they find themselves to be the victim and to report it at the earliest opportunity.
- All incidents, in conjunction with the anti-bullying policy, are investigated thoroughly.
- As with all bullying, staff will take a proactive role in educating children about the effects of bullying and what to do if they find themselves victim.
- Staff are aware of how offensive material can be removed from websites following the school's guidelines.
- If staff become aware of children using any online Social Media accounts, where they are underage and dates of birth have been falsified to enable them to gain access, this will be reported to the Provider.

7.5 Dealing with and Removing Offensive Content from Websites

- Always work within the guidance of the schools anti-bullying policy.
- Where online material is upsetting or inappropriate, and the person or people responsible are known, the quickest way is to ensure that the person who posted it understands that it is unacceptable and is asked to remove it.
- If the person or people responsible has not been identified, or refuses to take down the material, the SLT or Subject Leader need to contact the host. It is more than likely that the material will contravene the host's acceptable use policy. It is vital that a screenshot is taken before contacting the host and printed or saved in conjunction with the ICT, Online Safety and Data Protection Policies.
- In cases of illegal content the SLT must contact the police. In this case it is up to the police to decide what evidence is required.

ICT Policy

8. Introduction

ICT is changing lives of everyone. Through teaching ICT we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. ICT skills are a major factor in enabling children to be confident, creative and independent learners and functional members of society.

9. Vision

The Vision

Our vision has been formed with the use of Becta's ICT Quality Mark criteria.

Leadership and Management, Curricular, Learning and Teaching, Resources.

Make the application and use of ICT paramount to allow for virtual interactive classrooms, on – line access and remote access to curriculum and teaching materials. Keep data on the different groups of pupils so that, for instance, gender issues, the gifted and talented, pupils with special education needs, or those without home access to a computer can be tracked.

Extending Opportunities for Learning, Impact on Pupils.

Provision of ICT facilities will be fully incorporated into a classroom, rather than a centralised suite, to make ICT another fully integrated teaching and learning tool. It will also allow learners, teachers and others to communicate, move through their data, use resources and access teaching materials wherever they are. In addition. We will use ICT to share experiences of the teaching and learning in ICT .

Professional Development, Impact on Pupils.

Ensure that all staff harness the safe use of technology and use it confidently. Target development opportunities more carefully and systematically to match identified individual needs. Use a range of different training approaches, ie in-house training when appropriate, use of commercial organisations, local authority courses. Allocate time to share experiences of the teaching and learning in ICT.

10. Aims

10.1 To enable all children to use ICT with purpose and enjoyment:

by providing tasks which are interesting and give scope for individual responsibility.

10.2 To enable all children to develop the necessary skills to exploit ICT:

by ensuring enough access by pupils to become more proficient in the basic ICT skills and by providing time outside lessons for use by children who do not have computers at home.

10.3 To enable all children to become autonomous users of ICT:

by planning activities which allow children opportunities to apply their skills in a variety of different subject contexts.

10.4 To enable all children to evaluate the benefits of ICT and its impact on society:

by leading group or class discussion about the benefits and limitations of ICT and by creating opportunities to compare classroom use of ICT with that in the wider world.

10.5 To meet the requirement of the National Curriculum as fully as possible and enabling all children to reach the highest standards of achievement:

by intervening, where appropriate, to reinforce an idea or teach a new point. By selecting groups where all pupils are equally active and involved in the task, and have equal access to the computer keyboard.

by planning activities which allow different levels of achievement or incorporate possibilities for extension work.

10.6 To create the atmosphere and levels of resource to encourage all members of the school community to learn with ICT:

by raising the profile of ICT in the school and by providing a continuous programme of staff development.

11. Curriculum coverage and progression

11.1 Whole School Curriculum

- ICT will be fully integrated into all subjects across the curriculum.
- The nature of ICT as a tool means that there will be many opportunities for links with other subjects.
- Teachers will plan a wide range of activities that emphasise the development of ICT capability and others which support the subject being taught.

11.2 There are eight units of work to be covered over the course of two years. The years link to the stage at which skills are expected to be taught.

<i>Units Covered Yearly from Year 1 – Year 6</i>	
Coding and Computational Thinking	Art and Design
Spreadsheets	Music
Internet and Email	Databases and Graphing
Writing and Presenting	Communication and Networks

- The Computing subject leader will review teachers' Topic plans (termly) to ensure: a range of teaching styles are employed to cater for all needs, a clear progression of skills is planned for and to ensure the development of children's ICT capability.

11.3 Planning

- The schools Computing curriculum, which is based upon Lancashire County Council's Computing framework, will provide guidance on the skills and knowledge to be covered in each year group.
- Teachers will need to plan their work so that these skills are taught and that they are practised and developed during work in other subjects.
- Work planned for children will be relevant to them and their lives. It will build on their existing skills and provided opportunities to develop new ones.
- Wherever possible real data will be used, and the use of E-mail will be used to link with children in other countries and other cultures.
- The MediumTerm Planning of Computing, which should be closely linked to topic work, will consist of highlighted skills, knowledge and understanding in the schools Computing curriculum.
- The curriculum will then be passed onto the next teacher to ensure that all relevant skills are taught within each stage.
- Activities will be planned on teacher's individual topic plans.
- The main outcome for each series of lessons will be recorded on topic plans and assessed on the school's assessment spreadsheets.

11.4 Differentiation

- Activities using ICT will be planned to allow for different levels of achievement by pupils or to include the possibility of extension work.
- Teachers will be expected to intervene where appropriate to reinforce an idea or teach a new point.
- Topic planning is differentiated to meet the range of needs in any class including those children who may need extra support, those who are in line with average expectations and those working above average expectations for children of their age.

11.5 Teaching Strategies

- Children may be required to work individually, in pairs or in small groups according to the nature or activity of the task.
- Different pace of working.
- Different groupings of children - groupings may be based on ability either same ability or mixed ability.
- Different levels of input and support.
- Different outcomes expected.
- Pupils will have the opportunity to participate in a variety of activities to learn to use ICT and apply these skills in a meaningful context.
- They will also evaluate how ICT is used in everyday life and compare this with the way they use it in school through:
 - ✓ short directed activities to practice a specific skill
 - ✓ activities with a subject context to practice and develop skills previously learned
 - ✓ open ended activities which allow pupils to choose which tools to use or to select from a variety of media
 - ✓ whole class discussion to allow reflection on the use of ICT.
 - ✓ Teachers and support staff will ensure that they understand the skills and concepts to be taught and the role of discussion in developing a critical awareness of the use of ICT.

11.6 Learning styles and the Learning Environment

- People have preferred styles of learning. Learning opportunities must be provided in a variety of ways so that no learner is disadvantaged but motivated.
- Teachers are encouraged to plan learner-centred activities which encourage a process of active inquiry.
- Teachers plan for and use a range of teaching styles for example: visual, auditory and kinaesthetic.
- Teachers are provided with the resources to ensure they can employ a range of teaching styles.
- Medium term planning is monitored to ensure it takes account of differentiation and progression.
- When teaching, practitioners use open questions, differentiated activities and assessment for learning strategies which develop and challenge children's thinking and learning.
- In the classroom and ICT suite teachers are encouraged to create a stimulating learning environment.
- Examples of good work and skilled development are displayed.
- Key words are displayed in the ICT Suite, along with, key objectives and Online

- Safety information.
- Child friendly guidance and advice will be on display within the ICT room.

12. Assessment

12.1 Methods of Assessment

Computing is assessed both formatively and summatively using the Lancashire Framework for Computing teaching and learning.

12.2 Formative Assessment

Formative assessment occurs on a lesson-by-lesson basis based on the lesson objectives and outcomes in the school's Computing curriculum. These are conducted informally by the class teacher and are used to inform future planning.

12.3 Summative Assessment

- Summative assessment involves the use of Assessment for Learning in Computing. Assessment for Learning is embedded within the subject and teachers have a range of skills to deploy. For example, sharing clear objectives and success criteria, peer and group discussion, oral and written feedback, questioning, modelling success, positive and constructive dialogue etc Children are encouraged to evaluate their own and others' work in a positive and supportive environment.

12.4 Assessment Activities

- Activities are planned at the end of each unit of work which enable summative assessments to take place where children's Computing capability is assessed.
- This work is accompanied by a description of the context in which pupils completed the task and how it was undertaken.
- The work is assessed against the knowledge and understanding set out in the Lancashire Skills Framework.
- The teacher makes an assessment of each child and assesses the level of their ability and understanding at three different levels:
 - An excellent knowledge and understanding (can apply the taught skills independently)...
 - Some good knowledge and understanding (can apply the skills but may need revision and a small amount of support)...
 - Failed to make the expected progress (has grasped some/none of the taught skills)...

12.5 Recording of Assessment

- A spreadsheet is used to record details of the assessment activity along with teacher judgements.
- The judgements of teachers are supported through the end of unit work saved in the children's folders.

- Teacher's assessment is monitored each term and, as part of the monitoring, the school portfolio is updated.
- Information on children's Computing capability is shared with appropriate stakeholders, such as governors and parents, as well as, through display, celebration events, newsletters, reports and relevant websites.

13. Monitoring

13.1 Monitoring Teaching and Learning

Monitoring Computing will enable the Computing subject leader to gain an overview of Computing teaching and learning throughout the school. This will assist the school in the self-evaluation process identifying areas of strength as well as those for development.

In monitoring of the quality of Computing teaching and learning the Computing subject leader will:

- Scrutinise plans to ensure full coverage of the Computing curriculum requirements
- Analyse children's work
- Observe Computing teaching and learning in the classroom
- Hold discussions with teachers and pupils
- Teach Computing sample lessons
- Keep a portfolio of work samples
- Walk rounds
- Learning environments
- The subject leader will be responsible for providing informal and formal feedback to the Senior Management Team relating to the standards of Computing.
- Formal feedback will take place in the Summer Term and will be used to set priorities for the following academic year.
- There is an annual review of this policy by the Computing subject leader. A major review involving all staff, governors and other stakeholders will take place every three years.

14. Foundation Stage

14.1 Activities

- We fully understand that Computing is part of children's everyday lives. In light of this we ensure that Computing forms a vital part of children's education from the very beginning. Computing is an integral part of the classroom and learning in the Foundation Stage.
- Practitioners in the EYFS use the Curriculum Guidance for the Foundation Stage and the Creative Curriculum to plan learning opportunities for children.
- The teaching of Computing in the foundation stage incorporates child-led, teacher-led and open ended learning opportunities.

- The activities planned encourage children to become independent, discerning users of Computing, able to choose appropriate tools and explore the possibilities offered by technology.
- This gives the children the abilities needed to develop their schools in other years. Children also learn how to use Computing to explore, communicate and express their ideas and feelings.

14.2 Planning

When planning to use ICT, practitioners:

- establish what children already know, building on existing knowledge and experience;
- plan opportunities for children to use a range of stimulating ICT resources within the learning environment;
- use ICT to enhance existing learning opportunities;
- encourage children to talk about and during their experiences of using ICT;
- identify ICT in the world around us;
- model the use of ICT in a range of contexts, avoiding communicating adults fears and perceptions of the limitations of ICT to children;
- encourage parents to be involved in the use of ICT with children in the setting, at home and in the environment.

14.3 Resources

- ICT resources that are used in the Foundation Stage develop learners' skills and understanding.
- A short explanation of how resources work is given, similar to showing children how to play a game or use scissors during practical activities.
- Specialised resources which are simple enough for young learners to use and explore independently are deployed in the Foundation Stage.

14.4 Computers

- Where computers are used, attention has been paid to ensure that the area is suitable up for young children to use it.
- Appropriate furniture is provided so that children are comfortable.
- A lowercase keyboard is provided to support letter recognition and early writing.
- There is adequate space around the computer to allow children to use other resources (e.g. paper, pencils, books, small world equipment etc.) alongside it if they wish.
- The computers are situated within the normal learning environment. This places the computer, and therefore ICT, in a meaningful and familiar context for the children.
- The practitioners and Foundation Stage Leader ensures that the organisation of the computers facilitates independent use.

14.5 Organisation

- As well as providing appropriate resources, practitioners organise them effectively within the learning environment.

- Where possible resources are portable or regularly relocated within the learning environment.
- The organisation of resources and computers ensures that children are able to use the resources when they identify they would be useful.

14.6 Role Play

- The use of ICT within the role play area supports children's understanding of the functions of ICT in the world around them.
- The use of ICT in the role play area often includes real, pretend or home-made computers, telephones, fax machines, answer phones, mobile telephones, photocopiers, videos, televisions, cash tills, bar code readers, kitchen technology and household appliances.
- Practitioners model the use of this technology and encourage children to discuss how and why it is used.

14.7 Assessment and Progression

- Practitioners elicit information about children's everyday experiences of ICT at home and in their communities. This involves ongoing discussions with parents.
- Practitioners regularly observe children's engagement in activities involving ICT. They ensure that these observations inform future planning and provision and build upon children's interest.
- The assessment of ICT is recorded on the assessment sheets used by the other key stages. However, the spreadsheets allow practitioners to make notes on the child's progress. This builds up a picture of each child's ICT capabilities.

15. Equal opportunities and Inclusion

15.1 The National Curriculum

The National curriculum states that, "All pupils, regardless of race, class or gender, should have the opportunity to develop ICT capability."

- All children are entitled to equal access to all ICT equipment in order to develop their personal ICT capability.
- When children work in groups care will be taken to ensure that all children are active and have equal access to the computer or ICT resources.
- Where necessary, records will be kept of computer use to avoid dominance of any group.
- Children with a computer at home are encouraged to use it for educational benefit and parents will be offered advice about what is appropriate and how they can keep their children safe.
- Children will be encouraged to practice keyboard skills at home and develop proficiency.
- For pupils who do not have computers at home, there will be other opportunities to use a computer informally
- For example, Breakfast Club, Homework Club etc. Computer Club at lunch time and before school.

15.2 Special Educational Needs and Able Pupils

- Pupils with special educational needs will be entitled to the same access to ICT as their peers.
- When planning lessons teachers will identify the learning goals for the majority of children as well as extension and differentiated activities for the more able and SEN.
- Consideration will be given to modifying the task, or providing peer or adult support, for children with difficulty.
- It is important to note that pupils with learning difficulties may achieve well in ICT and should be given every opportunity to provide support for others.
- Teachers will liaise with the SENCO on the use of ICT to improve their involvement in the curriculum. For instance, to improve writing and presentation, to practice skills or to focus on the interpretation of graphs.
- We recognise ICT offers particular opportunities for pupils with special educational needs and gifted children.

Using ICT can:

- increase access to the curriculum
- raise levels of motivation and self esteem
- improve the accuracy and presentation of work
- address individual needs
- raise standards in Literacy and Numeracy
- equip children with vital life skills
- ensure equality.

16. Liaison and transfer between settings

- When liaising between key stages and classes, teachers are able to access Computing assessment for children on the shared network.
- At the end of Key stage Two children's ability is assessed but there is currently no system for liaising Computing ability on transfer to Secondary Education. The Secondary Schools with which we work do not require this information. This situation is constantly monitored so that we are able to provide this information in the future if it is deemed necessary.

17. Home, school and community links

- Children are given the option to complete some homework tasks, when appropriate, using ICT out of school.
- Teachers are sensitive to the fact that children may not have access to ICT or may not wish to use it to complete tasks out of school.
- Any work brought into school must be scanned for viruses.
- **Our school website, which is constantly being updated, helps to promote the school's achievements as well as providing information and communication between the school, parents and the local community.**

18. Resources

18.1 Deployment of Resources

ICT resources are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment across the whole curriculum.

18.2 ICT Suite and Classroom Computers

- To enable regular and whole class teaching of Computing the school has an ICT suite which all classes in Foundation Stage, Key Stages 1 & 2 use to develop their ICT skills.
- To support the cross curricular nature of ICT there are computers in the classrooms in both Foundation, Key Stage 1 and Key Stage 2.
- There is also a 'mini-suite' of computers in Key Stage One so that focused group work, in both Computing and other subjects, can be carried out.
- The computers in class and the suites are also used for additional cross-curricular and oneoff tasks.
- Individual machines in classrooms support the development of ICT capability by enabling further development of tasks from the ICT suite; encourage research, and allow for the creative use of ICT in topic work. This is highlighted in the Computing and topic plans.
- The school has also invested in a group set of iPads that can be used in class, Breakfast Club, Chill Zone and other relevant activities.
- Adequate consideration is given to the physical security of rooms containing ICT equipment (including associated cabling).

18.3 Interactive Boards

- All classes have Interactive Whiteboards and a consistent interface is provided on all machines and boards to enable familiarity and continuity with generic 'toolkit'.
- There is also an interactive whiteboard in the ICT suite and a data projector linked to a laptop in the hall, the laptop is used to incorporate ICT into worships and PE.
- Specialist equipment and spares e.g. sensors, are kept in the Subject Leaders Cupboard.

18.4 Software

- In accordance with the Lancashire ICT Security Framework, we understand that, all software, data and associated documentation produced in connection with the work of the school are the legal property of the County Council, which will normally hold it for the benefit of the school. Exceptions to this will be allowed for software and documentation produced by individual Teachers for lesson purposes – this includes schemes of work, lesson plans, and worksheets or as otherwise agreed in writing by the Headteacher.

18.5 Removal of Resources

- The System Manager (Headteacher) and Computing subject leader, in conjunction with the school technician, ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location.
- These arrangements take into consideration the risks associated with the removal and the impact these risks might have.
- Prior to the transfer or disposal of any ICT equipment the Headteacher, in conjunction with the Computing subject leader and school technician, ensure that any persona data or software is obliterated from the machine.
- The School uses Preston Recycling (01772 562411), as advised by Lancashire County Council, to support in the process of removing data if required.

18.6 Computers, laptops and equipment used by teachers, support staff and administration staff.

- Reasonable care is taken in the siting of computer screens, keyboards, printers or other similar devices.
- Wherever possible, and depending upon the sensitivity of the data, users observe the following precautions:
 - devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information.
 - Specific consideration is given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained.
- The school has a 'clear desk policy', i.e. hard copies of sensitive data are not left unattended on desks;

18.7 Inventory of Resources

The Headteacher, in accordance with the School's Financial Regulations, ensures that an inventory of all ICT equipment is maintained and all items accounted for annually.

19. Roles and responsibilities

19.1 Senior Leadership Team

The overall responsibility for the use of ICT rests with the senior management of our school. The Head, in consultation with Computing subject leader:

- determines the ways ICT should support, enrich and extend the curriculum;
- decides the provision and allocation of resources;
- decides ways in which developments can be assessed, and records maintained;

- ensures that ICT is used in a way to achieve the aims and objectives of the school;
- ensures that there is an ICT policy, and identifies an Computing Subject Leader.

19.2 Computing Subject Leader

- There is a designated Computing subject leader to oversee the planning and delivery of ICT within the school.
- The Computing leader will work with the school management team to ensure implementation of the school's ICT policy and Computing development plan.
- The Computing leader will be responsible for monitoring curriculum coverage and the quality of teaching and learning.
- The Computing leader will plan and lead the development of all school staff in ICT and provide regular reports on the level of resources.

The Computing subject leader will be responsible for:

- raising standards in Computing as a national curriculum subject;
- facilitating the use of ICT across the curriculum in collaboration with all subject leaders;
- providing or organising training to keep staff skills and knowledge up to date;
- to keep staff and the SLT up to date with online safety regulations and advice;
- advising colleagues about effective teaching strategies, managing equipment and purchasing resources;
- monitoring the delivery of the Computing curriculum and reporting to the Senior Management Team on the current standards in the subject;
- liaising with ICT technicians regarding the upkeep of software and hardware across the school;
- work in partnership with the subject leaders to ensure all National Curriculum statutory requirements are being met with regard to the use of ICT within curriculum subjects.

19.3 The Classroom Teacher

Even though whole school co-ordination and support is essential to the development of ICT capability, it remains the responsibility of each teacher to plan and teach appropriate ICT activities and assist the subject leader in the monitoring and recording of pupil progress in ICT.

20. Health, Safety and Security

20.1 As a school we recognise that health, safety and security are essential in the use of ICT.

- To ensure we fulfil current legislation we will operate all ICT equipment in compliance with Health & Safety requirements.
- The Headteacher, in conjunction with the Computing leader, is responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school.

- The governing body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.
- In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.
- Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided.
- In keeping with the Lancashire Schools ICT Framework the school will ensure that:
 - equipment, data and staff are adequately protected on a cost effective basis against any action that could adversely affect the school;
 - users are aware of (through the ICT user agreement) and fully comply with all relevant legislation;
 - the SMT and Computing subject leaders create and maintain, within the school, a level of awareness for ICT security. They emphasise the need for ICT security to be an integral part of the day-to-day operation so that all staff understand their own responsibilities in this respect.

20.2 Pupils Use of ICT

- Pupils using school equipment and the associated networks and systems are covered by the relevant 'Rules for ICT Users' and 'E-mail and Internet Use Good Practice' documents.
- Parents and pupils have agreed to abide by the rules set out on both these documents.
- Pupils are encouraged to close computers down and prepare them for use.
- Pupils have chairs of the correct height, eyes level with the top of the monitor screen, and are encouraged to sit comfortably and use both hands for the keyboard.
- Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers.

20.3 Legislation

- The Headteacher, in conjunction with the Computing subject leader, is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy.
- Teachers are made aware of relevant legislation and sign the Users Policy to show their understanding and compliance
- All staff are aware of relevant legislation including:

Data Protection Act 1998

The Data Protection Act exists to regulate the use of computerised information about living individuals. The 1998 Act is consistent with the principles established in the 1984 Act but extends the regulation to certain manual records as well as computerised information.

To ensure staff are compliant with this act the school advises that staff:

- do not store personal information (telephone numbers, address, dates of birth) about any adult or pupil, on school computers. All this information is stored, in keeping with the Data Protection Acts, on the administration system in the school office
- do not give out personal information on any child or adult to another person. For example, list of class names to a parent, phone numbers of one parent to another, details about staff
- if information (telephone numbers, address, date of birth, full name) is used on a document for the purpose of writing to parents, other professionals, reports, the person who writes the document should ensure that it is encrypted or protected by a password
- that when necessary, staff use MyLGFL to transfer documents between school and home rather than transporting laptops or using USB memory devices and disks
- understand that the school enforces a strict 'clear desk policy', i.e. hard copies of sensitive data are not left unattended on desks.
- Disposal of waste ICT media such as print-outs, floppy disks, magnetic tape, USB sticks etc. will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.
- Failure to comply with the provisions of the Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

Computer Misuse Act 1990

Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:

- unauthorised access to a computer system or data;
- unauthorised access preparatory to another criminal action;
- unauthorised modification of a computer system or data.

To ensure staff comply with this act the school:

- gives all users of the school system written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy
- assigns staff usernames and passwords to access the school network. Passwords are regularly changed. Passwords are changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur. The need to change one or more passwords will be determined by the risk of the security breach.
- users who forget their password must request the System Manager or ICT subject leader to issue a new password.
- advises staff and pupils on keeping usernames and passwords safe.

- Staff are made aware that failure to comply with these regulations may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

Copyright, Designs and Patents Act 1988

The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of “literary work” covers computer programs and data. Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or license.

To ensure staff comply with these regulations the school makes them aware, through a written agreement, that:

- all copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective license or contract.
- all users are given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

The Headteacher and ICT leader are responsible, in conjunction with Senior Management Team, for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licenses accord with installations.

The school is aware that it may be open to legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action has been taken to resolve the breach.

20.4 Misuse and Abuse Guidance

Users are responsible for notifying the Head teacher or Computing subject leader of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Internal Audit.

Where there is evidence of misuse or abuse that may necessitate disciplinary or possible criminal action exceptional care must be taken care must be taken to maintain the integrity of any computer evidence and the following guidelines implemented.

-

- Do not turn on or operate the subject computer, or try to access the data held on any computer media.
- Do not allow anyone else to touch the equipment.
- Contact Lancashire Audit Service Computer Audit Team alerting them of the suspicion and indicating the seriousness of the suspected incident. They will

advise you of the action to take and will contact the police if deemed necessary.

- If computer media is provided as evidence e.g. floppy disks, USBs, tapes or print outs, place it in an envelope or bag which is immediately sealed, signed and dated.
- This should then be stored and locked away until required by the computer investigator.
- Document who obtained the evidence, who secured it and who had control of it on the envelope.
- Keep the number of people who know of the suspicions to a minimum – all actions taken should be kept confidential.
- The original suspect may have accomplices or may be innocent of the allegations.
- Do not solicit the assistance of the resident 'computer expert'. The processing of computer evidence requires specialist knowledge, training and tools.

The Headteacher should allocate sufficient resources each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements in their role.

- Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data.
- A record of the training provided through the school to each individual user will be maintained.
- In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

20.5 Antivirus

- The school will always use appropriate Anti-virus software, as advised by the Local Authority, for all school ICT Systems.
- All users will take precautions to avoid malicious software that may destroy or corrupt data.
- The school ensures that every ICT user is aware that any suspect or actual computer virus infection must be reported immediately to the Headteacher or Computing subject leader who must take appropriate action, including removing the source of infection.
- The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.

21. Review

- Due to continuous developments in ICT, the Computing subject leader, Senior Management Team and Governing Body will officially review this policy each academic year.
- Every year the Computing Policy will undergo a comprehensive review.
- The next annual review will be July 2024

November 2023, Lily Ferguson