ST. GERARD'S
CATHOLIC PRIMARY SCHOOL

Computing and Online safety policy

Our Mission Statement

'With Christ at our side and St Gerard as our guide, we live, love, learn and pray together'

This policy covers the following areas:

- **Online-safety**
- **Curriculum Responsibilities and Infrastructure**
- **Internet / Mobile Phone/ Tablet use.**

Reviewed: May 2022
Next review: July 2023

St Gerard's Catholic Primary School
Computing Policy

Computing Statement of Intent

At St. Gerard's Catholic school, we aim to provide our pupils with the skills required to become competent, confident and creative users of information and communication technology. In our ever-changing world of technology, we recognise that computing is an integral part of everyday life: we use it on a daily basis, at home and at school. Our intent is that our pupils can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation. The overall impact is to develop independent learners who are equipped with the skills of analysing problems in computational terms and have repeated practical experience of writing computer programs in order to solve such problems.

Our intention throughout the school, is to ensure that our pupils are taught the importance of 'Online Safety' and they understand what they should do if they have any concerns. We are extremely proud that our pupils understand how to behave respectfully online. Our aim is for children to leave us with a positive attitude towards digital literacy.

Online-safety

1. Introduction

1.1 The governing body of St Gerard's Catholic Primary School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous online-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the Head Teacher to ensure that this policy is implemented, that updates in online-safety is given high priority across the school, that consultations on the details of the arrangements for online-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The governing body expects the Head Teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing body

3.1 The governing body will consider and ratify this online-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it: including participating in any relevant online-safety training if they use information and communication technology in their capacity as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children. We also have a link governor who liaises with the subject lead, to ensure the subject is being taught well across the school.

Head Teacher

3.3 The Head Teacher is responsible for ensuring that:

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this online-safety policy;
- the governing body is given necessary advice on securing appropriate information and communication technology systems;

- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;

- the school has a designated senior person to co-ordinate online-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated safeguarding lead (DSL);

- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;

- the school provides all employees with updates in online-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be;

- pupils are taught online-safety as an essential part of the curriculum, this is done through our PurpleMash computing scheme and links with our local PCSOs;

- the senior leadership team and all staff are aware of the procedures to be followed in the event of a serious online-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem;

- records are kept of all online-safety incidents (CPOMs) and that these are reported to the senior leadership team;

- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;

- there is appropriate supervision of, and support for, technical staff;

- any outside contractor, which manages information technology for the school, undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the Head Teacher commensurate with their salary grade and job descriptions;
- participating in training provided by the school and in consultations about this policy and about its application, including online-safety within the curriculum;

- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to;

- participate in training provided by the school and in consultations about this policy and about its application, including online-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.

- Users must not disclose their password or write it down. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

4.3 **Social Media**

Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract or that the school is, or will be, brought into disrepute.

Action will be taken if staff, parents/carers post inappropriate information related to the school including members of staff and children.

4.4 Cyberbullying

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When children are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety.

- Pupils will be taught about the effects of cyberbullying
- Pupils will be encouraged to keep any evidence of cyberbullying
- Pupils will be made aware that the police will be able to trace the originator of any messages
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported, will be recorded on CPOMs (DSL will be alerted). Sanctions can now be made for incidents that occur out of school.

5. Education and training

5.1 Education and training in online-safety will be given to staff.

5.2 The education of pupils in online-safety is an essential part of the school's online-safety provision and will be included in all parts of the curriculum.

5.3 The school will offer education and information to parents, carers and community users of the school about online-safety. The school website has online-safety links providing this information. To ensure that we reach people who do not have the internet, we write online-safety information on the newsletters and provide information on online-safety as part of the inspire workshops. The online-safety information provided as part of the inspire workshop is age related.

5.4 Suitable training will be provided through the school for all employees. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. As a school we use The national Online Safety programme, regular Prevent training and annual Safeguarding training.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of

the school's data protection policy, including the requirement for secure storage of information.

7. Technical aspects of online-safety

7.1 The school will seek to ensure that the information and communication technology systems, which it uses, are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the Head Teacher and senior leadership team with regular reports to indicate whether there have been any incidents.

7.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the Head Teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the Head Teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

8.4 As a school we use the DNA monitoring system. The DSL and the Headteacher receive updates via email of any inappropriate activity. Most often these hits are false positives, but are reviewed regularly.

Curriculum, Responsibilities and Infrastructure

1 - Intent

At St Gerard's we recognise and value the use of computing technologies as a teaching and learning tool for both children and adults and seek to encourage pupils to become autonomous and independent in their use. We aim to develop a whole school approach to computing and online-safety that ensures continuity and progression and which develops the following core beliefs:

We believe that the rapid development of technology in the home, the workplace and the wider community has had and will continue to have an immense impact on the lives of individuals. Children need to develop a variety of computing skills, which allow them to harness the power of technology and use it both purposefully and appropriately.

We believe that computing technologies are an important medium for learning and study at all educational levels and that, through the effective use of such technologies, pupils and adults may enhance and extend learning opportunities and provide a powerful and motivating means to improve attainment in all curriculum areas.

We believe that the effective use of computing technologies allows pupils to communicate their ideas in a creative manner that reaches out beyond the classroom and which carries with it ethical implications and consequences.

Our specific Aims for Computing are:

- To provide pupils with opportunities to develop their computing capabilities in all areas specified by the National Curriculum.
- To develop pupils' awareness of the use of computing technologies not only in the classroom, but also in everyday life.
- To allow pupils to evaluate the potential of such technologies and also their limitations.
- To provide pupils with a detailed understanding of how to use such technologies safely and in a manner that fits with the Catholic ethos of the school.
- To develop logical thinking and problem solving.
- To provide opportunities for pupils to gain knowledge about a wide range of computing tools.

2 – Implementation (Roles and responsibilities)

School will support the implementation of the computing curriculum in the following ways:

All Teaching Staff will:

- Ensure the safe use of equipment, manage computer access for pupils and actively teach required computing skills.
- Inform the Computing coordinator or Technician of any issues or faults arising with respect to computing equipment.
- Use computing technologies effectively to promote learning whenever it is appropriate to do so.
- Make use of the laptops and iPads whilst ensuring that pupils are aware of the protocols of their use.
- Ensure that the school's safety procedures are known, understood and implemented within their classroom and that children (and their families) are provided with the skills and knowledge to use computing technologies safely beyond the classroom setting.
- Ensure that all users do not import/download any objects/files or viruses onto any school owned/linked device that could pose a threat to the school network.
- To promote a positive image of computing technologies and ensure pupil's work is purposeful and appropriate and conducted with confidence and enjoyment.
- Be aware of specific issues where notified, e.g. shutdown procedures, recharging of laptops/IPads, file management, use of: digital cameras, video camera, calculators, TV, DVD player, CD players, Interactive whiteboards, roamers, projectors, visualisers, microscopes etc.
-

In order to achieve our declared aims with respect to Computing, the following roles and responsibilities should be observed.

The Computing Subject leader (Mr Wilson) will:

- Monitor the work in computing including assessment and recording. This will involve overseeing the development of a portfolio of exemplar work (available in each classroom) and assessments (staff assessments).
- Highlight areas for the development of computing.
- Take the lead in policy development and the integration of computing into schemes of work designed to ensure progression and continuity in pupils' experience of computing throughout the school.
- Monitor the use of resources and the budget accordingly.
- Work alongside the Office manager and SLT to co-ordinate the purchase of equipment.
- Encourage and facilitate systematic development of knowledge and skills of teachers, support staff and adult help, to enable them to fully support, access and use computing technologies.

- Keep abreast of current thinking by reading and attendance at courses.
- Take a lead role in the supporting the Digital leaders.
- Monitor the teaching of Online-safety across the school.

The Computing Technician (Michael Hartop of Logistix Computer Solutions) will:

- Install and build new computer systems as directed by SLT.
- Evaluate nature of any technical failures and following discussion with SLT may undertake necessary repairs.
- Ensure that all hardware and software is in good working order for use of children and staff.
- Support teaching staff in the setting up and organisation of equipment.
- Maintain anti-virus software updates ensuring that all equipment is protected from known virus attack.
- Monitor the backing up of files onto appropriate storage devices and will periodically run checks to ensure this process is running correctly.
- To routinely check desktop set-up / reimage the desktop to ensure that pc/laptop performance is maximised. Develop appropriate procedures to maintain the standard image assessable to students on iPads.
- Add and remove programmes to computers as necessary.
- Maintain the computer based register for all machines and use this to log ongoing changes.
- Routinely check the school's printers to ensure efficient use of resources and minimise downtime.
- Evaluate the efficiency of classroom computer performance; rebuild and reformat as directed by the SLT.
- Monitor computer-cabling systems within classrooms and inform senior management team or of any Health and Safety concerns.

The Computing Governor will:

- Ensure that the governing body meets its responsibilities in helping the school resource, plan and deliver a coherent and effective computing strategy.
- Support the school's strategic computing development and contribute to the school's vision for the future use of computing technologies.
- Raise awareness within the governing body of the use of technology within school.
- Contribute to the formulation of the school computing policy.

3 – Implementation (Planning and Delivery of Content)

At school, a pupil's entitlement to computing technologies will consist of three separate areas, though clearly interrelated and overlapping components.

(a) - As a discrete subject - The teaching of a specific programme of study for computing based upon the Programme of Study as outlined in the National Curriculum. This PoS focussed on three aspects of the computing curriculum; Online-Safety, digital literacy and programming skills.

The school currently follows the 'Switched on Computing' scheme of work for computing. All children between years 1-6 spend at least 40 minutes per week fulfilling the relevant task for that week. In addition to this, Year 3 and 4 spend 7 weeks working on Code.org.

In order to ensure delivery of this entitlement, the school provides 3 sets of 30 laptops and 6 iPads in each class.

Planning is provided as 'learning steps' within the switched on computing scheme of work. Staff are aware that each step may take more or less time depending on the children's ability level. Teachers make informal plans to adapt these learning steps routinely and the outcomes are measured in the teacher assessment proforma (monitored by the computing coordinator).

(b) – As discrete Online-safety lesson – Staff teach discrete Online-safety lessons, once every half term. The school follows the planning made available on the digital literacy website and they adapt this to their class. The planning ensures that there is full coverage of the different aspects of Online-safety and there is clear progression through the year groups. The staff update resources as and when required to meet the current Online-safety needs.

(c) - Supporting the broad curriculum – St Gerard's believes that Computing skills and knowledge are crucial aspects of all areas of the curriculum. Staff should use the cross curricular matrix to carefully consider opportunities in which computing technologies may complement learning objectives in other subjects and plan for their use accordingly.

There is also the provision of an interactive board in each classroom. These are available for multimedia presentations or interactive teaching programs.

Children are also encouraged to use computing skills at home to enhance their learning. Staff can recommend useful websites and have provided access to web based resources such as TT Rockstars and SPAG.com – pupils will have a username and password to access these at home.

Teaching and Learning

In order to implement good quality teaching, high standards of learning and good progress, staff should prepare lessons in line with the teaching and learning expectations. Teaching of computing will focus upon the teaching of objectives in sufficient breadth and depth, structuring them in a way that ensures good progression. Planning takes into account the need of all pupils to use computing technologies in appropriate contexts, throughout both Key Stages and will provide opportunities for pupils to experience a variety of learning strategies including; collaborative group work, investigative work, problem solving and enquiry-based learning. The use of computing technologies will be planned carefully and they will be differentiated to match the needs of individuals and groups of children.

Interactive technologies such as the classroom interactive whiteboards can enhance opportunities for learning when planned effectively.

4 – Impact (monitoring and assessment)

The overall impact is that children will be confident and independent users of computer technology. Teacher assessments of computing capability will be recorded throughout the year. Judgements of attainment should be completed against each lesson's learning objectives and used to inform future teaching. Summative judgements are made at the end of each unit of study using the stated learning outcomes. Formative assessment is used to guide the progress of individual pupils in their use of computing technologies. This involves identifying each child's progress, determining what each child has learned and what therefore should be the next stage in his/her learning. In the course of teaching, formative assessment is continually carried out in an informal manner. Summative assessment, are monitored by the computing coordinator in line with the monitoring and evaluation timetable.

Staff should encourage children to save examples of their work in the pupil shared area (Computing, Online-safety and cross-curricular). Teachers should keep examples of children's work and store this in the Online-safety and Computing portfolio. Work should be annotated by children (explaining what they have learnt during the lesson).

5 - Equal Opportunities & Inclusion

Computing activities should be planned and recorded to ensure that all children are given the same opportunity to use and develop their skills and knowledge in accordance with the equal opportunities policy.

Pupils with Special Educational Needs

Pupils with Special Educational Needs benefit from using computing technologies as it enhances access to the curriculum, and this in turn encourages motivation and the development of skills ensuring significantly higher achievements. Therefore, the opportunities to utilise such technologies should be maximised. Laptops and iPads are available to help support children with special educational needs. Pupils with Special Needs have the same computing entitlement as all other pupils and are offered the same curriculum.

Able children

Computing can be used to assist gifted and talented children both inside and out of school and to embed the school's aims with regard to developing excellence and enjoyment. Computing resources offer a wealth of material in readily accessible forms, which can be matched to the needs of individual children and enable them to develop a higher level of thinking skills.

6 - Community access and extended learning

Computing technologies can play a positive role in enabling or improving the transfer of information between pupil's homes and the school and may be used to allow students' learning to take place in an

extended home-school environment. At St Gerard's we are continuing to develop web-based learning resources. The Computing coordinator and SLT will work with staff to ensure home-school extended learning is available.

7 - Resources

The budget for computing is reviewed annually by the Head Teacher, following discussion with SLT, the Computing coordinator and Office Manager. It is based around a review of the impact of such resources upon teaching and learning. This is largely for hardware, core programmes and licenses, peripherals and consumables.

Software purchases will be approved for purchase by the SLT and Office Manager. Choice of "subject specific" software and budget control for the purchase of such software will be the responsibility of individual subject areas. All software purchased will be licensed to the school.

Staff need to ensure that each computer and peripherals are kept in working order, that all wires are safely tucked away and that a safe and tidy environment exists on and around the computer trolleys. Faulty equipment should be reported to the computing coordinator or the Technician for repair.

Laptops and iPads are maintained through a rolling replacement program. If further purchasing is required, Technician will work with the Office Manager and Head Teacher to achieve this.

8 - Professional Development

St Gerard's places a high priority upon staff professional development and recognises the importance of all staff remaining abreast of developments in computing. All eligible staff will undergo ongoing computing training including subject based training and Online-safety training wherever needs are identified.

9 - Management of information, transfer and transition

Management information system data is stored on the administrative server and is managed and updated by the School Business Manager. This is the central pupil data source and is backed up nightly. The system is supported by local authority technical services and is monitored by the Head Teacher. National data evaluation tools such as Asp are used in conjunction with the school's own tracking systems (STATonline) and are analysed by all teachers each term in line with the school's assessment and quality assurance policies. The school is committed to the reduction of administrative tasks through the effective use of computing technologies. The MIS data will be available for school transfer purposes wherever applicable and fully integrated within the LA-supported transfer protocols.

All staff accessing the school's pupil databases must be clear and mindful about data protection issues regarding access to such data.

The only remote access can be made available to teaching and administrative staff on a case by case basis, in order to facilitate out of hour work. This will always be authorised by the Head Teacher.

10 - Legislation

Staff should be mindful of appropriate legislation relating to computing technologies with respect to copyright and data protection issues.

11 - Child Protection and Internet Access

Using our computer network including the internet is an important aspect of information technology education. However, they present possible risks to the spiritual, moral and social development of pupils, particularly in terms of the nature of some of the material, which may be obtained via the Internet or sent by other devices. The school's Online-safety procedures will be reviewed annually in order to stay abreast of technological developments. It is essential therefore, that all are familiar with the procedures and that all pupil use of the network and in particular the school internet is governed by the school acceptable use policy. Further details are outlined in the Online-safety aspect of this policy.

Pupil use of the internet and email is governed by the schools' acceptable use policy.

12 - Health and Safety Procedures

The school recognises the need for proper risk assessment to be carried out with regard to the incorporation of computing across the broader curriculum. Health and Safety issues in computing include; taking care with setting up and moving equipment, establishing appropriate working conditions and general electrical safety. All equipment installation and subsequent use will comply with prevailing national and local Health and Safety guidelines and the school's Health and Safety procedures.

General Usage

Staff should be mindful of potential hazards and health concerns when using computing technologies. There should be sufficient space around any workstations for peripherals, paper, books and other materials to be used comfortably. Desk and floor space around workstations should be free of bags and coats, and gangways and exits must be kept clear at all times. When operating a workstation, pupils must look down at the screen with the top of the screen roughly at eye level. The mouse should be held lightly in the widest part of the hand with the pupils' fingers resting lightly on the mouse buttons so that a very small movement is needed to click a button. The arm or wrist should be supported on the table. In order to avoid eyestrain pupils should take a break from the computer at least once every 20 minutes and should not constantly lean their head forward. Pupils sharing a computer should be encouraged to make sure that everyone in the group can see without straining.

Multimedia Projectors

Pupils should be supervised at all times during the operation of multimedia projectors. Users should never stare directly into the beam of the projector and, when entering the beam, should not look towards the audience, or class, for more than a few seconds. If possible, users should keep their backs to the beam at all times.

Use of electrical appliances

It is imperative that all electrical equipment is kept in good working order. To ensure the health and safety of pupils and staff the following guidelines must be adhered to:

- Pupils should not be allowed to switch on the power at the mains.
- Equipment should be situated away from water.
- Pupils should always be supervised when using electrical equipment.
- All plugs, leads and equipment should be checked regularly and tested for electrical safety in accordance with Council guidelines.
- Computer systems will not be placed near magnets, radiators or have trailing wires, which can be tripped over.

13 – Anti-virus policy

St Gerard's Primary School's networked machines run Windows Defender, this is updated and checked on a regular basis. The technician will regularly check all computer drives in order to ensure that the network remains virus free, however data can be irretrievably lost through the actions of some viruses and staff will be updated periodically by the computing co-ordinator of any virus that is known to be a particular hazard to the school network.

In order to reduce the risk of a virus infiltrating a school computer the following protocols should be observed by all staff.

- All staff can now access planning using Google Drive, so there is no need for staff to transfer files into school systems via storage devices such as memory sticks or cards.
- Children should not introduce files or software from home into school systems without specific permission from a staff member who can run anti-virus checks on such files prior to their use.
- E-mail attachments present a particular danger of virus infection and should not be opened when the identity of the sender is unknown. Any e-mail that is received without the identity of the sender being known and / or a suspicious header or attachment should be deleted. If in doubt, either the Computing coordinator or Technician should be consulted prior to opening files.

14 – Laptop Computers for staff use

The use of laptop computers and iPad is to allow staff to extend their use of computing technologies to the home, allowing staff to be more flexible in their work. Microsoft Office software is installed, which allows word processing and desktop publishing to be carried out. The computers/iPads are registered for a particular teacher's own use but remain the property of the school and are covered by the school's insurance policy.

The software is licensed to the school, not to the individual user.

Copying of any software from the system is illegal.

No software should be installed or used on the computer without it being covered by the appropriate licence.

Internet / Mobile Phone/ Tablet use

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LA and DfES.

How will Internet use enhance learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

How will pupils learn to evaluate internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via SLT, computing co-ordinator or IT technician. This report should be logged on CPOMS. Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work. Developing a detailed understanding of online-safety is a key aspect of our whole school computing curriculum, something that is shared with and discussed with children of all ages at an age appropriate level as frequently as possible. Skills and understanding are built upon and developed across year groups. Children know to click on the 'Dolphin' (Hectors World) if they are unsure about the content of what they have searched for online.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Pupils can only send and receive internal emails unless specifically authorised.

How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Website or Twitter, particularly associated with photographs.
- In order to improve the school website and the ability to engage parents, consent is taken when a pupil starts at the school.

Video Conferencing and other Video Communications

Visitors/contributors may be invited to join (supervised) lessons through Skype or video conference in accordance with the visitor to School Policy. Pupils will not be allowed unsupervised access to video communications.

How can emerging Internet uses be managed and utilised?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. However, teaching staff will always build on any possible teaching points that arise in order to provide children with safe and open discussion opportunities; in order to prepare them for possible inappropriate material that they may come across outside of school. Network DNA sends an email to SLT if a keyword (that is potential unsuitable to view or indicates a potential risk to a child) has been typed into the computer. That member of staff can then assess the risk and take appropriate action.

How will filtering be managed?

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via SLT, the computing co-ordinator or IT technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later).
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

How will the policy be introduced to pupils?

- Rules for Internet access (including being responsible and safe) will be reiterated to children when they are using technology.
- Pupils will be informed that Internet use will be monitored.
- Online-safety and safe internet use are key aspects of the computing curriculum. Parents are involved and supported through inspire workshops, texts and newsletters.
- Pupils will be informed that Mobile phones should not be brought to school.

How will staff be consulted?

- All staff must accept the terms of the 'Responsible internet/ mobile phone /iPad use'

- All staff including teachers, supply staff, classroom assistants, support staff/any adult, will be provided with access to the School Computing Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff development/training in the safe and responsible internet use, and on school internet policy will be provided as required.

How will computing system security be maintained?

- The school computing systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Staff, are aware of expectations in regard to protecting network integrity and are informed of the expected practise in relation to the use of memory sticks and downloading files.

How should personal mobile phones/tablets be used within school?

Staff, are encouraged to ensure that all personal mobile phones/tablets are turned off during the school day. Where this is not feasible, staff must ensure that personal devices are always on silent. Staff, are not allowed to access social media through the school network and if personal devices are connected to the school network/internet then staff must be aware that they are using school equipment and the expected behaviour is just as it would be on any other school device.

If staff do not connect their mobile phones/tablets to the school network, then they may access website of their choosing during their breaks. However, if at any point, such access brings the school's reputation into disrepute (in any way) then staff disciplinary act will be undertaken which may result in dismissal and further legal action.

How will complaints regarding internet / mobile phone/ iPad use be handled?

Any complaint about staff/ other adults misuse must be referred to the Head Teacher. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions available include:
- interview/counselling by class teacher;
- informing parents or carers;
- removal of Internet or computer access for a period.
- warning/disciplinary action by Head Teacher

Depending on the seriousness of the incident – further more serious consequences may follow.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school computing policy in newsletters and the school prospectus. It will also be available on the school website.

- Information on internet use will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This will include demonstrations, practical sessions and suggestions for safe internet use at home in the form of inspire workshops.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents through the school website.

Review of the Computing Policy

Development, monitoring and review of the policy

This online-safety and computing policy has been developed, and will be monitored, by members of staff / governors that are responsible for computing and online safety:

- Headteacher (Mr Crehan)
- Deputy Head (TBA)
- Computing and Online-safety Co-ordinator (Mrs Nye)
- Website Co-ordinator (Mrs Breen)
- Online-safety and Computing Governor (Miss H Macilwraith/Mrs Nicholls)
- Designated Safeguarding Officer (Miss H Macilwraith/Mrs Nicholls/Mr Crehan/Mrs Powis/Mrs Kissun)
- Parent representative (TBA)
- Consultation with the whole school community has taken place with digital leaders, staff meetings, governors meetings, online-safety lessons, Inspire workshops, the school website and the school newsletter.

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Logs of internet activity
- Surveys of students, parents/carers and staff (including non-teaching staff)

The policy will be reviewed immediately where monitoring data shows a need. The policy will also be reviewed annually.

Appendices:

- Responsible Internet/Mobile Phone/Tablet Use. Rules for Staff, Supply Staff, Students or any Adults

Appendix 1

St. Gerard's Catholic Primary School
Responsible Internet/Mobile Phone/Tablet Use

Rules for Staff, Supply Staff, Students or any Adults

The school computer system provides Internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Social media should not be used through the school's information communication and technology systems. Staff should not have a social media presence with parents/relatives/carers of children in the school and action will be taken if staff are found to be communicating inappropriately about school business.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- Adults must not use personal devices (mobile phones or tablets) during teaching/ lesson time. Staff may use their mobile phones during their break times. We encourage staff not to join the school network.
- For the safety of staff, please refrain from using your mobile phone for taking photographs – you should use the school iPad or school camera.
- Memory sticks and other storage devices should not be used in school. Staff should save work on Google Drive.
- The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of websites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Staff, Student and any other Adult's Agreement I have read and understand the school Rules for Responsible Internet/Mobile Phone Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	***Date:***