

Sacred Heart RC Primary School, Kingsway, Rochdale, OL164AW



Sacred Heart RC Primary School

ICT and Acceptable Use Policy

February 2019



Contents:

Statement of intent

1. Legal framework
2. Curriculum
3. Assessment
4. Equal opportunities
5. Roles and responsibilities
6. Online learning and safety
7. Health and safety
8. Authorised use of facilities
9. Authorised use of communications facilities
10. Unauthorised use of facilities
11. Unauthorised use of communications facilities
12. E-mail policy advice to staff
13. Implementation of the policy
14. Monitoring and review



Statement of intent

Sacred Heart RCPS understands that ICT is an integral part of the national curriculum and that ICT skills are important to everyday life. Computers are a valuable resource in the classroom, benefitting the way pupils learn and helping teachers maximise their role as educators. In light of this, Sacred Heart RCPS is committed to ensuring that both staff and pupils have access to the necessary facilities to allow them to carry out their work. We believe that it is important for pupils and employees to be confident and competent users of computers and the resources they allow access to.

Signed by:

Sacred Heart RC Primary School, Kingsway, Rochdale, OL164AW



Love God, Love each other, Love Learning

_____ Headteacher Date: _____

_____ Chair of governors Date: _____



Legal framework

This policy has due regard to statutory legislation, including, but not limited to, the following:

- DfE 'Keeping children safe in education' 2016
- DfE 'Computing programmes of study: key stages 1 and 2' 2013
- Data Protection Act 1998

Curriculum

Sacred Heart RCPS aims to assist pupils in achieving attainment targets set out in the national curriculum. By the end of each key stage pupils are expected to know, apply and understand the matters, skills and processes specified in the national curriculum.

In accordance with the national curriculum, Sacred Heart RCPS aims to ensure that all pupils:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation.
- Are able to analyse problems in computational terms and have repeated practical experience of writing computer programs in order to solve such problems.
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically, to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

In key stage 1 pupils will be taught to:

- Understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions.
- Create and debug simple problems.
- Use logical reasoning to predict the behaviour of simple programs.
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content.
- Recognise common uses of information technology beyond school.



- Use technology safely and respectfully, keeping personal information private; identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In key stage 2, pupils will be taught to:

- Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solving problems by decomposing them into smaller parts.
- Use sequence, selection and repetition in programs; working with variables and various forms of input and output.
- Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the World Wide Web; and the opportunities they offer for communication and collaboration.
- Use search technologies effectively, appreciating how results are selected and ranked, and be discerning in evaluating digital content.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.
- Use technology safely, respectfully and responsibly, recognising acceptable and unacceptable behaviour and identifying a range of ways to report concerns about content and contact.

In order to give pupils, the best opportunity to learn these skills, each class will be allocated a time in computer rooms, to accomplish tasks and complete their work units.

Assessment

Teachers will record pupils' ability and progression through two types of assessment: formative and summative.

Formative assessment is carried out during lessons, based on objectives and their outcomes; these will be informally conducted by the ICT teacher.

Summative assessments are to be completed at the end of every term; pupils' capabilities are reviewed and a summative assessment is recorded on Target Tracker.



The Computing Lead then analysis these results and reports to the Headteacher and Governing Board within the Subject Leaders Position Statement.

Equal opportunities

Sacred Heart RCPS ensures that all children are provided with equal learning opportunities, regardless of social class, gender, culture, race, disability or learning difficulties.

In order to ensure pupils with special educational needs and disabilities (SEND) achieve to the best of their ability, outcomes are adapted and the delivery of the ICT curriculum is differentiated for these pupils; likewise, pupils who are gifted and talented and pupils with English as an additional language are catered for, as ICT can benefit the variety of learning styles that a class of children may have. Where possible, ICT is used to support SEND pupils, some software systems can be modified to aid language, spelling or reading development

Sacred Heart RCPS aims to maximise the use and benefits of ICT as one of many resources to enable all pupils to achieve their full potential.

Roles and responsibilities

Overall responsibility for monitoring the teaching of ICT throughout the school lies with senior management.

Senior management will make decisions on:

- How ICT should support, enrich and extend the curriculum.
- The provision and allocation of resources.
- The ways in which developments can be assessed, and records maintained.
- How ICT can benefit the aims and objectives of the school.

Senior management will also be responsible for overseeing the review of this ICT Policy with the subject leader and ICT Technician.

The subject leader will be responsible for monitoring the progression of teaching and learning. The subject leader is also responsible for:

- The implementation of the ICT Policy across the school.
- Maintaining resources and advising staff on the use of materials.
- Assisting senior management in deciding on the allocation of resources.

Sacred Heart RC Primary School, Kingsway, Rochdale, OL164AW



- Supporting teaching staff, advising and offering to share their expertise and experience.
- Leading staff training on new initiatives.
- Monitoring the quality and progression of teaching and learning.
- Helping staff in planning future lessons and assessments.

Classroom teachers will be expected to:

- Plan and deliver interesting and engaging lessons that adhere to the national curriculum.
- Provide equality of opportunity through their teaching approaches and methods.
- Keep up-to-date assessment records.
- Ensure pupils' development of skills and knowledge progresses through their learning and understanding of ICT.
- Set pupils suitable targets based on prior attainment.
- Maintain an enthusiastic approach to ICT.

An ICT technician will be available to maintain and keep equipment in good running order.

The ICT technician will visit the school once a week and any issues or broken equipment will be reported to them, the technician will also be responsible for:

- Adjusting access rights and security privileges in the interest of the school's data, information, network and computers.
- Disabling user accounts of staff that do not follow the policy and Acceptable Use Agreement, at the request of the Headteacher.
- Assisting staff with authorised use of the ICT facilities, if required.
- Assisting the Headteacher in all matters requiring reconfiguration of security and access rights, and in all matters relating to the ICT Policy.
- Monitor the computer logs on the school's network and report inappropriate use to the Headteacher.
- Accessing files and data to solve problems for a user, with their authorisation – if an investigation is required by the Headteacher, authorisation from the user is not required.



Parents will be asked to support the implementation of the ICT curriculum by encouraging their child's use of the computer at home. Parents will be made aware of e-safety through website updates and whole school events and will be encouraged to promote this at home.

When administering tasks to be completed at home, teachers will be sensitive to the fact pupils may not have access to a computer at home; these tasks will be optional.

Online learning and internet safety

Sacred Heart RCPS will offer a safe online environment through filtered internet access. We recognise the importance of teaching pupils about online safety and their responsibilities when using communication technology.

We will ensure that the use of filtering and monitoring does not cause "over blocking" which may lead to unreasonable restrictions as to what pupils can be taught.

Sacred Heart RCPS ensures the filtering systems in place will prevent children accessing terrorist and extremist material, in accordance with the school's E-security Policy and the Prevent duty.

At the start of each school year pupils will be taught about the potential dangers on the internet and about internet safety.

Pupils caught misusing or attempting to misuse technology and the internet will be reported to the Headteacher.

The ICT technician will keep the internet filters up-to-date, to avoid misuse.

Internet safety and cyber bullying talks and lessons will be delivered as part of the school's personal, social and health education programme.

Health and safety

All electrical wires and sockets, where possible, are kept out of the way of the pupils.

Pupils will be given a five-minute break if they're using the computer for more than two hours at a time.

The rules of the computer room will be displayed around the classroom and both staff and pupils will be expected to familiarise themselves with these

Authorised use of facilities

ICT facilities should only be used to complete school-related work. This includes, but is not be limited to:

- Preparing work for lessons, meetings, activities, reviews, etc.



- Researching for any school related task.
- Undertaking school-encouraged tuition, CPD, or for other educational benefit.
- Collating or processing information for school business.

Personal email accounts are only permitted if they have anti-virus protection approved by the ICT technician. Access to personal emails must not interfere with work duties.

Authorised use of communications facilities

The communication facilities provided by Sacred Heart RCPS should only be used as required by school-related duties. Authorised use of the communications facilities includes, but is not be limited to:

- Preparing work for lessons, meetings, activities, reviews, etc.
- Researching for any school-related task.
- Any school-encouraged tuition or educational use.

Unauthorised use of facilities

It is not permitted under any circumstance to:

- Use ICT facilities for commercial or financial gain, unless authorised in writing by the Headteacher.
- Physically damage the ICT facilities.
- Relocate, remove from the school, or otherwise interfere with ICT facilities without the authorisation of the ICT technician or Headteacher. Certain items are asset registered and security marked; their location is recorded by the financial assistant for accountability. Once items are moved after authorisation, staff are responsible for notifying the Business Manager of the new location. The exception to this is when items are moved to a secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. This password must be changed at regular intervals. User passwords must never be disclosed to or by anyone.

Sacred Heart RC Primary School, Kingsway, Rochdale, OL164AW



It is not permitted to use the ICT facilities at any time to access, download, send, receive, view or display any of the following:

- Any material that is illegal
- Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability, age, race or ethnicity
- Online gambling
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not users know them to be true or false
- Any sexually explicit content
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.

All users must not:

- Install hardware or software without the consent of the ICT technician or the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act 1998.
- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not – this is illegal.
- Purchase any ICT facilities without the consent of the School's Business Manager and Headteacher. This is in addition to any purchasing arrangements followed according to school policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet.



- Use the internet for any auctioning activity or to purchase items, unless given authority to do so by the Headteacher
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the Headteacher. This authorisation must be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal. This can include computer software, music, text, and video clips. If it is not clear that permission has been granted, or if the permission cannot be obtained, do not do so.
- Obtain and post on the internet, or send via email, any confidential information about other employees, the school, parents of pupils or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with responsibilities to supervise pupils.
- Use email or the internet for unauthorised purposes, this is likely to result in disciplinary action including summary dismissal.

Unauthorised use of communications facilities

It is not permitted under any circumstance to:

- Use the communication facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage the communication facilities.
- Use the communication facilities for personal use without authorisation from the Headteacher.
- Re-locate, remove from site or otherwise interfere with the communications facilities without the authorisation of the ICT Technician or Headteacher.

Use of the communication facilities is not permitted, at any time, to access:

- Any material that is illegal.

Sacred Heart RC Primary School, Kingsway, Rochdale, OL164AW



- Any material that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious beliefs, sexual orientation or disability) or any negative comment about other persons or organisations.
- Remarks relating to a person's sexual orientation, gender assignment, religion, disability, or age, race or ethnicity.
- Remarks, which may adversely affect the reputation or any organisation or person, whether or not users know them to be true or false
- Any sexually explicit material
- Any adult or chat-line phone numbers
- In addition, staff must not misuse the communication facilities in any way, including, but not limited to:
 - Using or attempting to use the school's communication facilities to undertake any form of piracy, including the infringement of media rights or other copyright provisions whether knowingly or not – this is illegal.
 - Using or attempting to use the school's communication facilities for internet or email access unless given authorisation by the Headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication regardless of ownership.
 - Copying, recording, or distributing any material from or with the communication facilities that may be illegal. This can include television media, films, telephone conversations and music. If it is not clear that users have permission to do so, or if the permission cannot be obtained, do not do so.
 - Using or attempting to use the communication facilities to call overseas without the authorisation of the Headteacher.
 - Using the communication facilities when it will interfere with teachers' responsibilities to supervise students.
 - Using the school's telephone facilities for permitted personal use for longer than 10 minutes. Should anyone need to use the telephones for longer than this, then authorisation must be sought from Headteacher. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls; however, the deputy head or Headteacher must be notified after the call. Any personal calls using the telephones maybe subject to a charge; this is at the Headteachers' discretion.



- Certain items are asset registered and security marked; their location is recorded by the administrative assistant for accountability. Once items are moved following authorisation, staff have a responsibility to notify the administrative assistant / business manager of their new location. The exception to this is when items are moved to the designated secure room for insurance purposes over holiday periods.
- If users are subjected to, or know about, harassment or bullying, users are encouraged to report this to the Headteacher.

1. Email policy – advice to staff

1.1. Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

2. Further guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use.
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.
- Remember, “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.



- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

Implementation of the policy

Staff are requested to report any breach of this policy to the Headteacher.

The Headteacher has the ability to Monitor all Inbound and Outbound emails from any school email account. Hard copies of emails can be used as evidence in disciplinary proceedings.

Use of the school's internet connection is recorded and monitored.

Random checks of asset registered and security marked items are carried out by the financial assistant.

The Headteacher checks computer logs on the school's network regularly.

Unsuccessful and successful log-ons are logged on all computers connected to the school's network.

Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

The ICT technician can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement the ICT Policy and to assist in any difficulties

The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.

The school's database systems are computerised. Unless the Headteacher grants permission, users must not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. This must not be disclosed to anyone.

Attempting to access the database using another employee's user account and password without prior authorisation from the Headteacher could result in disciplinary action, potentially including summary dismissal.

User accounts are accessible by the Headteacher and ICT technician. And can be done so at any time without the users permission.



Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

Users are required to be familiar with the requirements of the Data Protection Act 1998, and to ensure that they operate in accordance with the requirements of the Act. Employees must adhere to following rules as detailed in the act:

- Do not disclose any material about a person, including a pupil, without their permission.
- Such materials that include information about person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences will not be disclosed.
- Do not send any personal data outside the UK.

Monitoring and review

This policy will be reviewed every year by the ICT Technician, Computing subject leader and the Headteacher.

Any changes made to this policy will be communicated to all members of staff.

All members of staff directly involved with the teaching of ICT are required to familiarise themselves with this policy.

The scheduled review date for this policy is February 2020.