OUR LADY IMMACULATE CATHOLIC ACADEMIES TRUST

ST JOHN RIGBY PRIMARY SCHOOL

God's will be done through work and play, as we follow Jesus day by day

Policy

Status: Good practice
Date of Review: December 2025
Approved by: LAC (Governing Body) Date: December 2026
Date of Next Review: Autumn 2026 (or sooner if required)

Table of Contents	
God's will be done through work and play, as we follow Jesus day by day	
RATIONALE	
What are our Key Principles and Aims?	
POLICY INTO PRACTICE	
What are our roles and responsibilities?	
Purpose of Study and Aims	
The approach to the teaching of e-safety at St John Rigby Catholic Primary School	
Use of digital and video images	
Staff using work devices outside of school	
Data protection	
Pupils using mobile devices in school	
Communication technologies	
Resourcing and CPD	
MONITORING & EVALUATION	

WHAT ARE OUR KEY PRINCIPLES AND AIMS?

John Rigby is a community based upon the strong Catholic values of Faith, Hope, Forgiveness, Love and Trust. The ethos of our school is that it promotes inclusion and the valuing of each individual, encouraging self-esteem, self-discipline, and mutual respect.

Our mission statement lies at the heart of all we do and underpins our overarching core aims:

- To ensure ***God's* will** is achieved by empowering our children to develop as happy, safe, confident and successful learners who are able to make informed choices that are in their own and others best interests.
- To enable children to ***work*** with a joy and love for learning, acquiring the knowledge, skills and behaviours needed to make a positive contribution to society.
- To enable children to ***play*** with an inquisitive and exploratory mind as they imagine, collaborate and create. They will take ownership of their learning journey and know that limitations are also opportunities for growth, showing courage to sometimes be wrong.
- To inspire children to grow, ***day by day***, in their knowledge and understanding of the virtues to live by, reflecting our Gospel values of Faith, Hope, Forgiveness, Love, and Trust, whilst continuing to flourish and discover their unique God given potential.

Key contacts

School IT Provider	Easi Pc
Head Teacher	Mrs McGettigan
Online Safety Lead	Miss Guard
Designated Safeguarding Lead	Mrs McGettigan
Deputy Designated Safeguarding Leads	Mrs Ball Mrs Mcloughlin
Designated Safeguarding Officers	Miss Guard Mrs Parks Miss Ward

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St John Rigby school:

Local Academy Committee (Governors)

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The LAC has overall responsibility and that reporting to Governors will include a review of filtering and monitoring, detailing activity in relation to online safety 'incidents'.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the St John Rigby's school community, though the day to day responsibility for online safety will be delegated to the Online safety Lead, who is a part of SLT.
- The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and that support given to those who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- ensure that the filtering and monitoring provision is reviewed and recorded at least annually.
- liaises with commissioned external IT service providers
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

Online Safety Lead

- Meets with the Designated Safeguarding Lead as and when appropriate
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies and associated documentation
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place through training and advice for staff.
- liaise with curriculum subject leads to ensure online safety is mapped, embedded and evaluated
- Reports to LAC Governors to review effectiveness of monitoring the Online Safety practices
- receive regularly updated training to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: content; contact; conduct: and commerce.

Easi PC:

Easi PC is responsible for ensuring:
• that the St John Rigby's school school's technical infrastructure is secure and is not open to misuse or malicious attack
• that the St John Rigby's school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
• that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
• that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online safety Lead / Officer for investigation / action / sanction
• that monitoring software / systems are implemented and updated as agreed in St John Rigby's school policies

Teaching and Support Staff

Teaching staff are responsible for ensuring that:
• they have an up to date awareness of online safety matters and practices outlined in this policy
• they have read, understood and signed the Staff Acceptable Use Policy (AUP)

• they report any suspected misuse or problem immediately to the Online Safety Lead or a member of SLT
• all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official St John Rigby's school systems
• All online safety best practice is embedded in all aspects of the curriculum and other activities
• Pupils understand and follow the online safety and acceptable use policies
• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
They understand the responsible use of AI, when created resources to support teaching and learning.
• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
• in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection / Designated Safeguarding Lead

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

*They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The DSL should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying

The role of Pupils

All pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents / carers would sign on behalf of the pupils.

All pupils –

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Need to understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school.

The role of all staff and volunteers

All staff and volunteers are responsible for –

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Locking computers / devices at times such as breaks to ensure there is no leaking of data.

The Role of Parents / Carers

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

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website records in accordance with the relevant school Acceptable Use Policy.
- Notifying a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites. We will regularly inform parents and carers of websites they can use for this, including:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

Purpose of Study and Aims

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The purpose of a school e-safety policy is to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents and carers, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

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

St John Rigby Catholic Primary School will demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. Our e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The approach to the teaching of e-safety at St John Rigby Catholic Primary School

Regulation and technical solutions play a critical role in e-safety. Additionally, St John Rigby Catholic Primary School recognises the importance of educating pupils to take a responsible approach to their use of technology.

E-safety education will be provided in the following ways:

Our curriculum will reflect the importance of e-safety by embedding it across all areas of learning, including the Computing curriculum, PSHE, and, where appropriate, within other subject areas.

Key e-safety messages will be reinforced as part of a planned programme of assemblies and teaching times.

Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line.

Pupils will be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
Staff will act as good role models in their use of ICT, the internet and mobile devices

In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the relevant person can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

In Key Stage 1, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private.
Identify 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:

Use technology safely, respectfully and responsibly.
Recognise acceptable and unacceptable behaviour.
Identify a range of ways to report concerns about content and contact.

By the end of Year 6, pupils will know:

That people sometimes behave differently online, including by pretending to be someone they are not.
That the same principles apply to online relationships as to face-to-face.
Relationships, including the importance of respect for others online including when we are anonymous.
The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
How information and data is shared and used online.
How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
The safe use of social media and the internet will also be covered in other subjects where relevant.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. St John Rigby's school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

Staff:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g on social networking sites.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the school's policies concerning the sharing, distribution and publication of those images. Those images should only be taken on the school's equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the St John Rigby's school into disrepute.

Parents:

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. Due to Safeguarding, we would not permit any video or group photos of pupils.

Pupils

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the St John Rigby's school website.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Staff using work devices outside of school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's term of acceptable use, as set out in the acceptable use agreement for staff, governors, volunteers or visitors. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school, including in public spaces.
If staff have any concerns over the security of their device, they must seek advice from the school's IT provider.

Data Protection

There is an Olicat Trust policy for Data Protection. Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Pupils using mobile devices in school

Pupils in UKS2 (Years 5 and 6) may bring mobile devices (not smartphones) into school, under the following conditions:

- Parents have read and sign the mobile phone policy.
- The mobile device is not a smartphone.
- The mobile device is handed in to their class teacher upon arrival at school, and can be collected at the end of the school day.

Communication technologies

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Head Teacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website, Facebook or Class Dojo and only official email addresses should be used to identify members of staff.

Resourcing / CPD

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

- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, staff PD sessions, Inset training).
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

Reporting to Parents and Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's on-line experiences. Parents and carers often either underestimate or do not realise how often children and young people come across

potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will provide information and awareness to parents and carers through:

- Letters, Safeguarding monthly newsletters, school website, Class Dojo, Facebook

Monitoring agreements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years. At every review, the policy will be shared with the governing board.