Online Safety Policy

Policy Approved/Updated	September 2025
Policy Review Date	September 2026
Reviewer	Amy Marriott

Part of OUR LADY OF LOURDES CATHOLIC MULTI-ACADEMY TRUST

Nottingham Diocese Multi Academy Trusts CATHOLIC SCHOOLS Moving Forward Together

Contents

Our Mission Statement

At St Joseph's we pride ourselves on our mission statement: 'Growing in Love, in the Spirit of Christ, for the benefit of all'.

We feel our Mission statement 'Growing in Love, in the Spirit of Christ, for the benefit of all' reflects all we stand for as a community. We put the example of Christ at the centre of all we do to help us grow socially, academically, spiritually, morally and physically in our learning and our friendships. We do this for ourselves as well as for the members of the school, parish, local, national and international communities in which we live.

Our Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

Scope of the Policy

This policy applies to all members of St. Joseph's School community (including staff, students, pupils, volunteers, parents/carers, visitors) who have access to and are uses of St. Joseph's School technology systems, both in and out of the school.

The Education and Inspectors Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are both on and off St. Joseph's School site and empowers members of staff to impose consequences for inappropriate behaviour. This is pertinent of incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the online safety policy, for reviewing the effectiveness of the policy and holding the head teacher to account for its implementation.
The governor who oversees safe-guarding and online safety is Maeve Tombs.
The role of governors will:

- Ensure that they have read and understood this policy
- Regularly monitor online safety incident logs
- Report to relevant governors meetings
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

Head Teacher and Senior Leaders

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
The Head Teacher and (at least one) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation.
The Head Teacher and 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 Head Teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

The Designated Safeguarding Lead

Details of the school's DSL (Mrs Broad, Mrs Wilkins-Campbell and Mrs Jordan) are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL and Online Safety lead (Mrs Marriott) take responsibility for online safety in school, in particular:

- Takes day to day responsibility for online safety issues.
- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and follow the steps outlined in the filtering and monitoring guidance.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing board

This list is not intended to be exhaustive.

ICT Technical Staff

The ICT Technical Staff are responsible for:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Ensuring 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.
- Ensuring that the use of networks/internet/digital technologies is regularly monitored in order that any misuse or attempted misuse can be reported to the Head Teacher and Senor Leaders.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any online safety incidents are logged on CPOMS and follow the steps outlined in the filtering and monitoring guidance.

This list is not intended to be exhaustive.

Teaching and Support Staff

All staff are responsible for ensuring that:

- The maintain an understanding of this policy
- The implement this policy consistently
- They have an up to date awareness of online safety matters
- They have read, understood and signed the staff acceptable use policy
- Pupils follow the acceptable use policy
- They work with the DSL and Online Safety Lead to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and the filtering and monitoring guidance.
- Any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

Students/Pupils

Students/pupils are required to:

- Use the school digital technology systems in accordance with the pupil acceptable use agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the filtering and monitoring system.

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. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, the school website, social media and links to organisations and websites. Parents and carers will be encouraged to support the school in promoting good online safety practice

Parents/carers are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy.

- Ensure that their child has read, understood and agreed to the terms on the acceptable use policy (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and Members of the Community

Visitors and members of the community who access school systems or programmes will be expected to read this policy, when relevant, and follow it. If appropriate, they will be expected to sign the acceptable use policy.

Educating Pupils About Online Safety

The education of pupils in online safety and digital literacy is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum and will be routinely recapped within the teaching of the computing curriculum. The online safety curriculum is broad, relevant and provides progression.

Online safety should form a fundamental part of child protection and safeguarding measures and you are encouraged to think of appropriate times during the timetable where these sessions could be delivered – this could be at the start of your computing lesson or at another point during the week. However, these sessions cannot be blocked together and should be threaded throughout the curriculum, across the whole school year.

We now use 2BeSafe on Purple Mash to deliver our online safety provision. This has been split into the core areas of online safety:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

Each of these units are used from Reception to Year 6. Each session within the framework is designed to last 15-20 minutes.

By the end of primary school, 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.

Educating Parents About Online Safety

Many parents and carers have only a limited understanding of online safety risks, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours.

The school will raise parents' awareness of internet safety through:

- The sharing of this policy
- Letters/newsletters
- Weekly online safety guides
- The school website
- Parents Evenings
- High profile events such as Safer Internet Day
- Reference to the relevant websites, www.swgfl.org.uk, www.saferinternet.org.uk, www.childnet.com/parents-and-carers

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL and Online Safety Lead.

Concerns or queries about this policy can be raised with any member of staff or the head teacher.

Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class through e-safety starters and online safety units.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL and Online Safety Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to read and agree to an acceptable use policy with regards to use of the school's ICT systems.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Pupils Using Mobile Devices in School

Pupils may bring mobile phones into school under special circumstances (e.g. children in year 6 who walk home alone). These must be switched off and handed in to the school office on arrival and collected upon leaving school at the end of the day. Pupils must not use their phones in school

Any use of mobile devices in school and any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff Using Work Devices Outside 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 terms of acceptable use.

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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and Internet acceptable use policy
- Curriculum policies; such as: Computing, PSHE and RSE
- Confidential reporting code

Acceptable Use Policy for EYFS and KS1

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Acceptable Use Policy for KS2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or trusted adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision • Bring a personal mobile phone or other personal electronic device into school without prior permission. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Acceptable Use Policy (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking we have parents permission. • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**