St Mary of the Angels E-Safety Policy

"Recognising and celebrating the presence of Christ in one another".

Mission Statement

Recognising and celebrating the presence of Christ in one another.

At St. Mary of the Angels:

- *we aim to follow Jesus through the teaching of the Gospels and inspire each other to be Christ-like;*
- *we all work as a big team to encourage everyone to be the best that they can be, at work and at play;*
- *we create a safe, positive, fair environment where all feel respected and valued.*

Reviewed April 2022

Contents

1. Aims

Our school aims to:

- Have strong processes in place that protect pupils, staff, volunteers and governors when working online.
- Deliver an effective approach to online safety, which allows us to protect and educate the whole school community in its use of technology.
- Establish clear systems to identify, intervene and escalate an incident, where appropriate and necessary.

2. Legislation and guidance

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

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (September 2021), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

- Searching, screening and confiscation at school

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

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of St. Mary's, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St Mary of the Angels 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring the policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitoring online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Mr Gerry Wintrip, Safeguarding governor.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and internet.
- Commit to training and CPD to keep abreast of the KCSIE requirement linked to E – Safety for children in schools

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy through regular, up-to-date and appropriate training, and for ensuring that it is being implemented consistently throughout the school. The headteacher is also the designated person for child protection and is trained in dealing with online safety issues

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our **Safeguarding and Child Protection Policy**.

Our current DLS is Claire O'Hara and our Deputy DSLs are Elizabeth Smith, Emma Hayes and Frances Murray

The DSL takes lead responsibility for online safety, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager, Computing Co-ordinator and other staff, as necessary to address any online safety issues or incidents.
- Ensuring that any online incidents are logged and dealt with appropriately in line with this policy.
- 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 headteacher and/or governing board.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Having an up to date awareness of online safety matters and of the SMA Online Safety Policy and practises.
- Implementing this policy consistently.
- Agreeing and adhering to the terms in the Staff Acceptable Use Policy/Agreement (AUP) ,staff code of conduct and teaching standards, when using the school's ICT systems and internet.
- Ensuring that pupils understand and follow the Online Safety Policy and acceptable use policies.
- Reporting any suspected misuse or problem to the headteacher or Online Safety Officer so that it can be logged and dealt with appropriately in line with this policy.
- Ensuring that all digital communications with pupils, parents or carers are on a professional level and are only carried out using official school systems.
- Embedding online safety issues in all aspects of the curriculum and other activities.

3.6 Parents and carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use their internet/mobile devices in an appropriate way. St Mary's will take every opportunity to help parents understand these issues through parents' evenings, newsletters, websites and

information about national/local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

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

- What are the issues? UK Safer Internet Centre
- Hot topics – Childnet International
- Parent factsheet – Childnet International
- Advice by age – Internet Matters

3.7 Pupils

Pupils are expected to:

- Adhere to this policy, the Acceptable Use Agreement and other relevant policies.
- Ask for help from school staff if they are concerned about something they or a peer has experienced online.
- Report online safety issues in line with the procedures in this policy.

4. Educating pupils about online safety

4.1 Teaching and learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school, children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks.

Pupils are taught about online safety in every year group at SMA, using a planned progressive online safety curriculum, based on the Dfe guidance document published in June 2020 'Education for a Connected World.' It is provided as part of Computing/RSE and is regularly revisited throughout the year.

Covering the key strands of:

- Online Relationships
- Online Bullying
- Self-Image and Identity
- Online Reputation
- Managing Online Information
- Health, Well-being and Lifestyle
- Privacy and Security

- Copyright and Ownership.

Additionally, all schools have to teach the following elements alongside the current guidance:

Relationships education and health and education in primary schools

Relationships and sex education and health education in secondary schools

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.

Pupils in **Key Stage 2** 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 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.

The safe use of social media and internet will also be covered in other subjects where relevant. Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Teachers and staff use Twitter to model the safe use of social media, this may take place on a school or personal device, please refer to the school social media policy.

Where pupils undertake searching of the internet, staff encourage children to use child-friendly search engines and monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches, this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

The school will use assemblies and events, such as ‘Safer Internet Day’, to raise pupils’ awareness of dangers that can be encountered online and may also invite trained speakers to talk to pupils about this; where appropriate as a way of enhancing the embedded online safety curriculum.

4.2 Rules for keeping safe

Underpinning the ICT curriculum are the SMART rules, which are reinforced in school across the curriculum:

- **Safe** – encourages young people to be safe by not giving out their personal details online.
- **Meeting** – draws attention to the risks associated with meeting someone you only know online.
- **Accept** – highlights the risks of accepting emails, pictures and text messages from unknown sources.
- **Reliable** – is a reminder that not all information found online is necessarily reliable.
- **Tell** – encourages children to tell someone if something happens or they meet someone online that makes them feel uncomfortable, or if they or someone they know is being bullied online.

These rules are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.

5. Educating parents/carers about online safety

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

- Regular inclusion of material in newsletters or other communications home such as 'eschools'. Additional information will also be available via the school website.
- Involvement in high profile events/campaigns such as Safer Internet Day
- Providing copies of pupils' Acceptable User Agreements
- Reference to relevant websites, publications and quizzes
- Opportunities to speak to staff and seek further advice during parents' evening

This policy will also be shared with parents.

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

Concerns or queries about this policy can be raise with any member of staff or the headteacher.

6. Cyberbullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is repetitive, intentional harming of one

person or group by another person or groups, where relationship involves an imbalance of power.

6.2 Reporting and recording online incidents

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues are reported to the DSL. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the Headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend.

We encourage children to take responsibility for protecting each other.

Staff are committed to recording examples of online bullying alleged or proven, on CPOMS.

The strategies used for sanctioning, supporting, identifying and communicating such incidents are outlined in our Anti bullying and Behaviour Policies

6.3 Managing incidents

In the event of suspicion of an infringement of policy then all the following steps should happen:

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images including youth produced imagery, nudes and semi nudes, as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

Websites visited by pupils, staff, volunteers, governors and visitors (where relevant) will be monitored to ensure they comply with the above

8. Technical Issues

Walsall Council Schools ICT support provides technical guidance for Online safety issues for all Walsall schools. The school IT provider provide support for technical issues in school on a daily basis and coordinate with Walsall Council. Technical support visits the school once every two weeks.

The IT providers responsibilities include : – antivirus updates and maintenance, network security, ensuring appropriate back ups, ensuring updates are regular and completed, managing and maintaining filtering and monitoring installation. This is not an exclusive list but outlines the main responsibilities

9. Filtering and monitoring

The Walsall Council school internet service is provided by Net sweeper and monitoring is carried out using Smoothwall Monitor via the Walsall Council Online monitoring service. Internet access is filtered for all users by Walsall Council. Illegal content (child sexual abuse images) is filtered by actively employing the Walsall Council. Content lists are regularly updated and internet use is logged and regularly monitored. However, we are aware that no filtering and monitoring is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence, teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that "over blocking" does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools. The school reports issues through logging a call to the service desk. Any filtering requests for change and issues are also reported immediately to the technical team. Requests from staff for sites to be removed from the filtered list must be approved by the Head teacher and this is logged and documented by a process that is agreed by the Head teacher. Test my filtering - http://testfiltering.com/test/

The school are currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. This is being implemented by Walsall Council Online Monitoring service by:

- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Walsall Council to support the school by drawing attention to concerning behaviours, communications or access
- ability to produce reports on the websites visited by all young people and adults using our systems
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up

- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail

10. Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Please look at the GDPR policy for further information on this

11. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them on school premises as the school provides access to technologies which can be used for learning. Mobile devices are handed in at the start of the day and are stored in the office. They are then collected at the end of the day and handed back to pupils.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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 confiscation of their device.

Watches that ink with any form of socail media are not permitted in school, as outlined in the school prospectus and Behaviour Policies

12. Staff

10.1 Staff using work devices outside school

Members of staff using a work device 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.

All our systems are accessed via an individual log in. Staff must ensure that their work device is secure and password-protected, using a combination of letters, symbols and numbers. Staff are encouraged to change these regularly and to never share their passwords for any IT system that they are responsible for. Access to systems is through groups so that only the relevant group of users can access a resource.

Staff must take 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.

Work devices must be used solely for work activities.

10.2 Staff mobile devices in school

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. Mobile phones may be used in staff room or offices where children are not present, but this use should be minimised. The desired option is for phone calls to be made outside of the school building or in the staff room or designated offices. The only exception to this is in case of emergency during a school trip.

Staff do not use their own mobile phone to take images of children, for example on a school trip, as the school has devices available for this.

10.3 Staff use of the school phone

Staff have access to the school phone in order to upoad and record videos or compliations of work. The schoolphone is storred safeyl in the Office Managers Office and is returned there once staff have finished with it.

Our Social Media Policy identifes the safe use of staff's personal devices in the school environment

11 Internet and Network access

11.1 Visitors to school including Governors

Visitors and governors cannot gain access to Wifi on personal devices.

11.2

11.3 Staff access

Staff can access the school Internet via a school devices and should not access the school wifi on personal devices.

13. Communications Technologies

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.

Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.

Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site (Governor Hub) that governors can access to via a personal user account.

Personal email addresses, text messaging, public chat and social networking programmes are not being used for communications with parents/carers and children.

Personal information is also not posted on the school website.

14. Personal Social Media use

Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.

Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community

Personal opinions are not attributed to the school

Security settings on personal social media profiles are regularly checked to minimise risk

Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.

14. Use of Digital Images and Videos

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, or newsletter. Photographs published anywhere that include

pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.

- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- 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 this is not covered by the General Data Protection Regulation. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.
- Pupils' work is only published with the permission of pupils and parents / carers.

12 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific intent, and will be proportionate. This will be recorded on CPOMS

Where a staff member misuses the school's ICT systems or internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures listed in the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. This will be documented by the HT or the AHT in the HT 's absence, confidentially. THis will then be available evidence to share with Governors and to identify next steps, in line with the Disciplinary Policies. Code of Conduct, Grievance or Whistleblowing Policies

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police or MASH.

13. Training

All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- An audit of online safety training needs of staff is carried out regularly, during this training process.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The online safety lead receives regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.

- The online safety lead provides regular guidance and training to support individuals where required.

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils and staff.

14. Monitoring Arrangements

This policy will be reviewed annually by the DSL and Computing Lead, and will be shared with the governing board.