Date ratified at Directors Board meeting	Review
15 July 2019	TLS Committee

St John the Baptist Catholic Multi Academy Trust

THE MAT MISSION STATEMENT

Our family of schools is united in the belief that God's love, peace, truth, and joy is for all. We are dedicated to the achievement of excellence in all we do. We cherish the uniqueness of each of our school communities and celebrate together as one Trust family. By following Jesus' example we bear witness to the greatness of God.

'To think, to feel, to do' *Pope Francis*

St John the Baptist Catholic MAT
Company No: 7913261
Registered Office: Surrey Street, Norwich NR1 3PB

ONLINE SAFETY AND ACCEPTABLE USE POLICY

IN TRAN communication for all

If you need this document in large print, audio, Braille, alternative format or in a different language please contact the Company Secretary on 01603 611431 and we will do our best to help.

Contents

.....

1. Aims

St John the Baptist Catholic Multi Academy Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, Directors 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy.

3.2 The Governing Body

Individual Governing Boards have the responsibility of holding their Headteacher/Head of School to account for the implementation of the policy.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

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 the internet (appendix 2)

3.3 The Headteacher/Head of School

The Headteacher/Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.4 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL), deputy and other Designated Safeguarding Officers are set out in each school's child protection and safeguarding policy.

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

- Supporting the Headteacher/Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher/Head of School, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher/Head of School and/or governing board

This list is not intended to be exhaustive.

3.5 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 and contact online while at school, 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
- 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 (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any safeguarding concerns arising as a result of online use are reported the DSL, and that assistance is provided for any investigation as necessary.

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency 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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1A and 1B)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher/Head of School of any concerns or queries regarding this policy
- Ensure that at an appropriate age, their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1A and 1B)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- Thinkuknow - age appropriate guidance on internet safety and safe surfing for young people, parents and professionals
- the National Crime Agency Child Online Exploitation and Protection command (CEOP)

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

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

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Head of School.

6. Cyber-bullying

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 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.)

6.2 Preventing and addressing cyber-bullying

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 tutor groups, and the issue will be addressed in assemblies.

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.

All staff, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 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.

6.3 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Governors are expected to abide by the terms of an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

However, staff are permitted limited use of the school's internet for non-work purposes, provided this would not bring their professional role into disrepute, and is in line with the MAT's Code of Conduct policy.

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 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them (or headphones) during school hours, unless they are a Sixth Form student, or unless they are directed to do so by their teacher as part of educational activities.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1A and 1B).

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.

9. 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, as set out in appendix 2.

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 password-protected, and where they contain personal data, 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.

10. 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 the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

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, e-bulletins and staff meetings).

The DSL and other Designated Safeguarding Officers will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed annually in the first instance by the MAT Operations Manager, and biannually thereafter. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to each school's:

- Child protection and safeguarding policy
- Behaviour policy

and to St John the Baptist Catholic Multi Academy Trust's

- Code of Conduct policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1A: Acceptable Use Agreement (Primary School pupils and parents/carers)

S 

I will only use the Internet and email with an adult.

A 

I will only click on icons and links when I know they are safe.

F 

I will only send friendly and polite messages.

E 

If I see something I don't like on a screen I will always tell an adult.

Students are bound by the AUP Agreement as part of their enrolment in the school. As and when it is age appropriate students are expected to learn about, read and discuss this agreement with their teacher, parent or carer, and the student must follow the terms of this agreement.

All parents, carers and students are bound by the terms of this AUP Policy and Agreement by their enrolment at a school within the St John the Baptist Catholic MAT.

Appendix 1B: Acceptable Use Agreement (High School pupils and parents/carers)

.

Acceptable Use Policy (AUP) Agreement – Students

• IT - in all its forms - is part of our daily life in school.
• This agreement makes students aware of their responsibilities when using IT in all its forms.
• All students have a school IT account which is for their **sole** use only and for which they are responsible.
• All pupils must abide by these guidelines, including any variations as may be made from time to time.
• All new students will have reference to this document as part of the enrolment form and process.
• All current students will acknowledge it as part of using their IT accounts annually or be taught about it in lessons in an age appropriate manner.

Any concerns or queries should be discussed with the Headteacher or the online safety coordinator.

Scope
This agreement applies to all students at the school and their use of personal and school owned devices. This is designed to keep students safe. The school Behaviour Policy sanctions will apply as necessary for any deliberate misuse of IT.

1. I will make sure that all my IT communications are responsible and sensible. I will be responsible for my behaviour when using the Internet. This includes resources I access, and the language I use.
2. I will only use IT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
3. I will only log on to the school network or other resources with my own user name and password. I will not
4. I will not reveal my passwords to anyone, or let anyone else use my account.
5. In school I will only use my school email address as the only email account used for any communications on school issues.
6. I will exercise caution when deciding whether or not to open any attachments in emails, or to follow any links in emails. If in doubt I will check with a member of staff before opening any attachments or links.
7. I will report problems that I have to the school via my teacher or an IT Technician.
8. I will let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
9. I will treat school IT equipment with respect. I understand my parents may be asked to pay for equipment that I damage.
10. I will not download or install software on school technologies. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I come across any such material I will report it immediately to my teacher.
11. I will not give out any personal information such as name, phone number or address.
12. I will adhere to any online safety training or guidance I have received. I will not arrange to meet someone offline unless this is part of a school project approved by my teacher, or without adult supervision.
13. Images of students and / or staff will only be taken, stored and used for school purposes in line with school policy and with appropriate parental and/or student consent. They will not be distributed outside the school network without this consent and with the permission of the class teacher.
14. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress, nor bring the school into disrepute.
15. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

16. I will respect the privacy and ownership of others' work on-line at all times.
17. I will not attempt to bypass any security on school systems, or make use of material that is not intended for student use.
18. I understand that all my use of the computers, the internet and other related technologies can be monitored and made available to my teachers or parents.
19. If I connect a mobile device (e.g. laptop or USB device) to the school network or a school device, I agree to the school systems accessing that device and that they may take necessary action.
20. If I bring a personal mobile phone or other personal electronic device into school, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material, or use inappropriate language when communicating online.
21. If I bring a personal mobile phone or other personal electronic device into school, I will not use it during the school day, unless my teacher instructs me to use it for educational purposes. This restriction applies to all pupils, except Sixth Formers who are allowed to use their mobile phones responsibly.
22. I understand that along with all personal property I may bring on site, that the school cannot be held responsible for the loss, theft or damage to any personal mobile phone or other personal electronic device I may bring into school.

Students are bound by the AUP Agreement as part of their enrolment in the school. As and when it is age appropriate students are expected to learn about, read and discuss this agreement with their teacher, parent or carer, and the student must follow the terms of this agreement.

All parents, carers and students are bound by the terms of this AUP Policy and Agreement by their enrolment at a school within the St John the Baptist Catholic MAT.

Appendix 2: Acceptable Use Agreement (staff, Directors, Governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, Directors, Governors, volunteers and visitors

All staff, Directors, Governors, volunteers and visitors are bound by the terms of this AUP Policy and Agreement by their employment within, voluntary support of or use of any ICT equipment at a school within the St John the Baptist Catholic MAT.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- 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
- Attempt to install any unauthorised software; if I want to use services or software I will inform the ICT Services Team and follow their guidance prior to any implementation.
- Share my password with others or log in to the school's network using someone else's details

I will use the school's ICT systems and access the internet in school, or outside school on a work device, primarily for educational purposes or for the purpose of fulfilling the duties of my role.

However, staff are permitted limited use of the school's internet for non-work purposes, provided this would not bring their professional role into disrepute, and is in line with the MAT's Code of Conduct policy.

I agree that the school will monitor the websites I visit.

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.

It is a condition of employment, voluntary work within or even use of ICT as a visitor within any establishment or school within St John the Baptist Catholic MAT that this AUP and Agreement is adhered to at all times by staff, volunteers and visitors.

Appendix 3: Online Safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, Governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you use a complex password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Online Safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**