| Date ratified at Full Board meeting | Review |
|---|---|
| **23 March 2026** | TLS Committee |

# ONLINE SAFETY AND IT ACCEPTABLE USE POLICY

## THE TRUST MISSION STATEMENT

*Inspired by the life of Christ we provide an exceptional education in our Catholic schools which enables our children:*

- to fully embrace all possibilities
- to flourish
- to develop their faith

*and therefore to choose a path that enables them to be a positive influence upon our world.*

'Prepare the Way' *The Gospel of St Mark 1:3*

**St John the Baptist Catholic Multi Academy Trust**

**Company No: 7913261**

**Registered Office: Surrey Street, Norwich NR1 3PB**

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
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## 2. 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
- Meeting digital and technology standards
- 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 DfE'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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

- Having effective monitoring strategies in place that meet their safeguarding needs.

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)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND) because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 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, as well as relevant job descriptions.

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 and governing board to ensure that the procedures within this policy are implemented, updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Trust IT Services Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher/Head of School, Trust IT Services Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### 3.5 The Trust IT Services Manager

The Trust IT Services Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

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)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to the DSL and the Trust IT Services Manager
- Following the correct procedures by seeking authorisation from the Trust IT Services Manager if they wish to bypass the filtering and monitoring systems for educational purposes
- 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.7 Parents/carers

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

- What are the issues? – UK Safer Internet Centre

- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet
- Healthy relationships – Disrespect Nobody
- 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.

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026).

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

**All** schools have to teach:

Relationships education and health 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
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults

- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

**Secondary schools** insert:

In **KS3**, 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 **KS4** 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

By the **end of secondary school**, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice

- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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.

### 4.2 Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 5. Educating parents/carers about online safety

The school will raise parents/carers' 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/carers.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

## 6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL or other member of the senior leadership team.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated 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, the staff member should reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Undermine the safe environment of the school or disrupt teaching, and/or
- Break any of the school rules, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or Headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Behaviour policy

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

### 6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

St John the Baptist Catholic Multi Academy Trust recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St John the Baptist Catholic Multi Academy Trust will treat any use of AI to bully pupils in line with each school's anti-bullying and/or behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school or Trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with the Trust's guidance on the use of Generative AI in schools.

## 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 Trust'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

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members 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 Trust IT Services 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, the 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 for staff, governors and volunteers

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).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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 Trust Compliance Manager. 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.
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 create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate.
12. I will not give out any personal information such as name, phone number or address.
13. 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.
14. 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.
15. 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.
16. 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.

17. I will respect the privacy and ownership of others' work on-line at all times.
18. I will not attempt to bypass any security on school systems, or make use of material that is not intended for student use.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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 (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 my private email account (if I am a member of staff) or other non-school communication system (e.g. WhatsApp) to conduct school business – instead I will use my school provided email address or communication systems (e.g. Teams).
- Communicate with pupils if they are not using approved school email accounts or systems, except to request them to use approved methods of communication
- 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
- Take photographs of pupils (unless I am a member of staff taking pictures on school business)
- Share confidential information about the school, its pupils or staff, or other members of the community other than in a work capacity
- 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 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 Trust IT Services 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:** |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| 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** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix 5: Policy on internet filtering

## 1. Policy Overview

- This filtering policy covers the schools in St John the Baptist Catholic Multi Academy Trust.
- The filtering policy is reviewed annually by the Trust IT Services Manager and the Designated Safeguarding Lead (DSL), and also at any other time deemed appropriate due to changing circumstances. During this process any feedback from each school's DSL will be reviewed.
- Significant policy changes identified at any point will be referred to the Trust's Executive Team for approval.
- The policy will be ratified annually by the Board of Directors.

## 2. Reasons for filtering internet traffic

- To protect the Trust and school networks against malware and overloading.
- To meet the Trust and schools' statutory obligations (e.g. Keeping Children Safe in Education KCSiE, the Prevent duty etc)
- To protect pupils against unsuitable material.
- To preserve the Trust and school networks for educational purposes.
- To protect the Trust and each school's reputation.

## 3. Overview of Filtering

- All school broadband traffic passes through filters provided by a supplier who is a member of the Internet Watch Foundation (IWF).
- At a minimum, all school internet filters block access to illegal Child Abuse Images (by actively implementing the IWF Uniform Resource Locator URL list) and integrating the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'. These filters for illegal content cannot be disabled by the school.
- The filters otherwise meet the current Department for Education standards for filtering.
- All Trust and school owned devices are subject to filtering whether on or off network.

## 4. Monitoring

- The school filtering systems log all internet access for all users.
- The logging systems are capable of identifying access by individual users.
- The logging systems can generate alerts over matters of concern or safeguarding.
- A log of alerts will be examined at least weekly by a designated team or individual at each school, and any concerns will be passed on to the school's DSL.
- The logs may be examined at any time by an authorised person.

## 5. Limitations of Filtering

- It is impossible for any filtering system to be 100% accurate in filtering and not filtering material. There is often no clear dividing line between such material, and attempts to over filter will result in much legitimate material being blocked and seriously degrade the academic value of the internet connection.
- The Trust recognises the limitations of any filtering system.

## 6. Types of Material Filtered

**Types of Sites and Material Blocked for All Users**

- Hacking or security threats
- Adult / pornographic content
- All categories covered by KCSiE

**Types of Sites and Material Blocked for Pupils**

- Generative Artificial Intelligence (AI)
- Social Networking
- Chat Sites
- Non-educational Games
- Violence (including self-harm)
- Intolerance
- Drugs and Substance Abuse

Where the individual school filtering system allows, schools may choose to add filters according to their needs, provided they consult their IT Service provider and they do not otherwise violate this policy.