St Bede's Catholic Voluntary Academy

E-Safety Policy

We commit ourselves to love, respect and serve one another as disciples of Jesus Christ

Contents

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of pupils
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of the Academy and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the Academy are able to use technology in a safe and responsible manner.

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. It is rare we do this; we ask students to delete harmful images or message or involve the police. Parents are advised to contact the police where peer on peer abuse is persistent under the Malicious Communications Act.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this 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 monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Jackie Kelly

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.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

3.3 The designated safeguarding lead

Details of the Academyl's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on a secure system 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 Academy's behaviour policy
- 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 and contact online while at the Academy, 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 Academy's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on a secure system 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:

- 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 and ensuring that pupils follow the Academy's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on a secure system and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's Rewards and Consequences policy

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

4. Educating pupils about online safety

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

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 and PSHCE to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this when relevant.

5. Educating parents about online safety

The Academy will raise parents' awareness of internet safety in the parents' newsletter, via text, and in information via our website. 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 raised with any member of staff or the headteacher.

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 Rewards and Consequence policy and Child Protection and Safeguarding 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 Academy 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 (Safer Internet Day), PSHCE and ICT lessons.

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

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy 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

Academy 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. It is rare that the Academy will search student phones; we will ask students to delete images or refer to the police.

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 are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendix 1). Use of the Academy's internet must be for educational purposes only.

We will monitor the websites visited by pupils to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendix 1.

8. Pupils using mobile devices in the Academy

Pupils may bring mobile devices into the Academy, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Any social times

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Academy's behaviour policy, which may result in the confiscation of their device. Mobile phones are expected to be turned off at the Academy entrance and not used for any purpose during the day. If a mobile phone is visible, staff will confiscate the phone and contact parents/carers. Failure to comply with this results in the Academy consequence system being implemented.

9. How the Academy will respond to issues of misuse

Where a pupil misuses the Academy's ICT systems or internet, we will follow the procedures set out in the Rewards and Consequences policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

10. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on a secure system. This policy will be reviewed every two years by the headteacher. At every review, the policy will be shared with the governing board.

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Rewards and Consequences policy

Approved: March 2019

Review date: March 2021

Appendix 1: acceptable use agreement (pupils and parents/carers)

St Bede's Student ICT Acceptable Use Policy.

All students at St Bede's Catholic Voluntary Academy must abide by, and sign, this user agreement regarding use of all aspects of ICT at St Bede's. Failure to sign this document will result in the student concerned not being able to access ICT facilities at St Bede's.

This document covers various areas relating to appropriate use of the network, internet, email and how the school will treat your child's data with respect and in accordance with the Data Protection Act (1998) and the upcoming General Data Protection Regulation (2018).

Whilst a student at St Bede's I will:

- not use ICT facilities to commit illegal activities, including relating to copyright infringement/piracy, discussion of illegal activities, accessing materials relating to drugs, pornography, extreme violence or terrorism
- not use any other user's account under any circumstances
- protect my password at all times and never share it with anyone
- not use school ICT to access social networking sites, including Facebook, Twitter, Instagram, or similar
- install any software, including games, without the express permission of my ICT teacher and/or the ICT technician
- not attempt to use any USB sticks/drives as they may contain viruses
- not attempt to bypass the school's internet filtering system
- not sending threatening, obscene, violent or otherwise rude/inappropriate messages or pictures to anyone
- not attempt to 'add' or interact with members of staff via social networking sites
- not send spam messages/email large groups of people
- report anything I see which is inappropriate immediately to a member of staff

I accept that, in the interests of child protection and complying with e-safety laws, the school has the right to:

- view details of all documents I have saved on school devices
- view any emails I send using my school account
- track my internet usage and the websites I visit using school facilities
- discipline me for any breaches of this policy

The school reserves the right to withdraw ICT access if pupils are found to be breaking this policy. Should this occur, alternative arrangements will be made for them to complete work relating to ICT.

Student name: _____ Signed: _____

Parent name: _____ Signed: _____

Date: _____

STUDENT MOBILE PHONES AGREEMENT

I accept that the school's policy is for mobile phones to be switched off and remain in bags during the course of the school day (8.40am - 3.05pm).