Saint John Houghton Catholic Voluntary Academy
Online Safety and Acceptable Use Policy (AUP)
March 2025

Foreword by the Headteacher

This policy has been agreed by the Governors and applies to everyone associated with the Academy Community; teaching staff, students, support staff, supply staff and guest users.

We rely on the internet and electronic communications both in and out of the Academy and so we are all responsible for the safety of our young people when using these media.

The Governors have asked me to distribute this policy and to ensure that everyone understands their obligations and responsibilities. Please take time to read through this document and then sign and return the relevant Code of Conduct.

As ever we value your support in safeguarding our young people and thank you for your cooperation.

S. J. Brogan

Mr S Brogan
Headteacher

BACKGROUND

1. This policy and the associated codes of conduct for staff and students have been compiled to safeguard students and all users of ICT at Saint John Houghton Catholic Voluntary Academy. This policy is part of our suite of safeguarding policies and procedures which are available to view or download from our website www.stjohnhoughtonilkeston.srscmat.co.uk

TEACHING AND LEARNING

Why the internet and digital communications are important

2. The internet and digital communications are essential elements in 21st century life for education, business and social interaction. The Academy has a duty to provide students with internet access as part of their learning experience. Internet use is part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

3. The Academy internet access is designed expressly for student use and includes filtering appropriate to the age of students. Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff and students. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation.

Students will be taught how to evaluate internet content

4. The Academy will ensure that the use of internet derived materials by staff and by students complies with copyright law. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

MANAGING INTERNET ACCESS

Information system security and filtering

5. The Academy ICT system security will be reviewed regularly. Virus protection will be installed and updated automatically and regularly. Security strategies will be adopted in line with latest best practice.

6. The Academy will work in partnership with the firewall provider and the internet filtering provider to ensure that filtering systems to protect students are in place and regularly reviewed.

7. The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Academy network. The Academy cannot accept liability for any material accessed, or any consequences of internet access. Parents/carers will be informed when inappropriate sites have been accessed and if deemed necessary by the Designated Safeguarding Lead the Police may be informed.

E-mail and social networking

8. Staff and students may only use approved e-mail accounts on the Academy system. Approved e-mail accounts are those provided by the internet service provider and set up by the Academy ICT staff. Academy business and communication between staff and students must not be conducted using e-mail addresses other than those specifically approved by the Academy.

9. The Academy will control access to social networking sites and consider how to educate students in their safe use. Students will be advised never to give out personal details of any kind which may identify them, their friends or their location. Staff and students will be reminded that social networking sites are public areas and that they should not bring the school into disrepute through their use.

MONITORING ICT SYSTEMS AND INTERNET ACCESS
Monitoring

10. The Academy has a right and obligation to monitor all ICT activity both on and off site where remote access has been granted. Monitoring will, for the most part, be automated. However, teaching staff are authorised to monitor student activity using RM Tutor & Senso when in the classroom and ICT staff will also use RM Tutor or Senso as part of technical support with the knowledge and permission of the user. Monitoring of staff activity outside of this remit will only take place when specifically authorised to investigate technical issues, possible breaches of this AUP or when investigating illegal activity. Any activity that is suspected may lead to this AUP being contravened or that may bring the Academy into disrepute will be investigated and may result in disciplinary action in line with the Academy Trust Disciplinary Policy for staff or in line with the Behaviour policy for students.

11. The information that may be extracted about any user's activities includes but is not limited to:

    - What PC they logged into the network from
    - When they logged in / out
    - What files they have created, looked at on the network and when
    - What files they have printed, through which printer and when
    - When they have changed their password
    - Who e-mails have been sent to / received from and the subject, message and attachments
    - What websites have been visited, how frequently, for how long and any files downloaded or viewed
    - What search terms were entered, and which search engines were used

12. Copies may be made and retained of e-mails and data and the school will disclose these if required in accordance with the Freedom of Information Act 2000.

Handling Complaints

13. Complaints of internet misuse by students will be dealt with by the Assistant Headteacher for Behaviour and Attitudes. Complaints about staff misuse will be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with the Child Protection and Safeguarding Policy.

14. Where illegal activity is suspected then the police will be involved.

COMMUNICATING E-SAFETY

Introducing Online-Safety to students

15. Students will be informed that network and internet use will be monitored. Students will be informed about the acceptable uses of ICT.

16. Online Safety will be delivered specifically as part of the Curriculum in Computer Science and PHSE.

17. All students will be required to sign agreeing to the Code of Conduct. They are also required to accept a digital version of the latest Code of Conduct every 42 days when they attempt to log onto a computer.

Staff and the Acceptable Use Policy

18. All staff will be issued with a copy of this policy, including the Code of Conducts for both staff and students and will be reminded that network and internet traffic will be monitored.

19. Staff will be reminded that phone or online communication with students can occasionally lead to misunderstandings and that professional relationships must be maintained at all times.

20. Staff will be required to sign a Code of Conduct governing use of the Academy ICT resources prior to the release of their ICT credentials.

Parents' / Carers' Support

21. Parents and carers will receive a copy of this policy individually on entry to the Academy and a copy will be posted on the Academy website.

AUTHORISING ACCESS

22. Students and their parents/carers will receive a Code of Conduct which must be signed and returned to the main office before using any school ICT resource.

23. The Academy will maintain a current record of all staff and students who are granted access to the Academy ICT resources.

FURTHER INFORMATION

Nominated Governor:	**Mrs C Gabriel**
Persons responsible for Online Safety:	**Mr S Brogan**
Head of ICT:	**Mr S Timms**
Online Safety:	**Designated Safeguarding Lead**
Network Manager:	**Mr J Reeks**