ICT SYSTEMS ACCEPTABLE USE POLICY EMPLOYEES, GOVERNORS & VISITORS

Date approved by Trust Board:	06th March 2020
Version:	05
Date revision approved by Trust Board:	
Publication Scheme:	Internal Trust Intranet
Next Review Date:	July 2022
Policy Owner:	Head of ICT

1. Audience

1.1 This policy is aimed at any person who is given access to any of the Trust's ICT computing, network systems or devices including, but is not limited to staff, visitors, including supply teachers, temporary staff and governors.

1.2 This policy does not apply to pupils, a separate policy and procedure is in place.

2. Purpose

2.1 The purpose of this document is to outline appropriate and inappropriate use of all ICT Systems including, but not limited to Network, Computer Systems, Internet, Email and mobile/portable digital data storage systems at Nicholas Postgate Catholic Academy Trust.

2.2 Whilst it is important that the policy target audience are able to use technology and related services effectively and flexibly, they must ensure that, when doing so, they do not make themselves vulnerable. This must also be balanced with the duty of the Headteacher and the Governing Body to safeguard children and the reputation of the Trust.

3. Policy Statement

3.1 This policy outlines the standards that the policy target audience are required to follow when using Trust ICT systems and the action that will be taken in respect of any breaches of this policy.

3.2 The policy aims to:

3.2a Reinforce the need to use the ICT systems safely and securely.

3.2b Ensure that the policy target audience are aware of the risks associated with the inappropriate use of the ICT systems.

3.2c Safeguard the policy target audience in connection with the use of the Trust ICT systems and to ensure they do not put themselves in vulnerable situations.

3.2d Ensure that the Headteacher, Trust Board, the LGB and the policy target audience maintain their duty to safeguard children and the reputation of the School and the Trust.

4. Scope

4.1 This policy applies to the policy target audience who have access to NPCAT ICT systems. The policy target audience are expected to comply with this policy and behave responsibly and professionally at all times whilst using the Trust ICT systems.

5. Requirements

5.1 This policy must be read and agreed to by the policy target audience before the use of any ICT equipment or login of user accounts.

6. Definitions

Sensitive Data	This includes but is not limited to confidential documentation regarding pupil behaviour, pupil attendance, pupil personal details, pupil special needs, pupil's parental details, and data held concerning staff, visitors or governors.
Portable Equipment & Mobile Data Devices	This includes but is not limited to laptops, tablets, mobile phones, smart watches, USB memory sticks, DVDs, CDs, external hard drives, MP3/4 players, mobile phones and other digital data storage devices.
MIS System	Management Information Systems including but not limited to Sims.Net, Bromcom, Scholar Pack and Arbor.

7. Responsibilities

7.1 The **Trust Board, and Headteachers** will ensure that all staff are made aware of this policy and any other related ICT protocols. This policy must be easily accessible to staff and new staff should also be made aware of the policy during their induction process.

7.2 The **Trust** must ensure that this policy is implemented across schools and that both current and new employees have access to, and are made aware of, this policy.

7.3 The **LGB, Headteachers & Line Managers** must be fully aware of this policy and ensure that they and all employees are aware of the policy and their own responsibilities. Employees must be made aware of the risks of using the Trust ICT systems and the possible implications to their employment if there is any inappropriate use.

7.4 The **HR Team** must provide advice where necessary to support the Trust, LGB and all staff when required, particularly where any disciplinary procedures may need to be instigated.

7.5 The **policy target audience** must behave responsibly and professionally at all times in connection with the use of the Trust ICT systems; both within the school & Trust, outside of work and must comply with this policy and cooperate fully with the school & Trust management in ensuring the implementation of this policy.

8. Your Computer and Network Account

8.1 Your network computer account allows access to sensitive data across numerous ICT systems. In order to maintain a high level of safeguarding and security, accompanying procedures are in place to ensure that everyone with access uses the account safely and responsibly.

9. Internet

9.1 The Internet is used as an invaluable tool for teaching and learning to enrich and extend the learning activities for all. Staff are responsible for defining appropriate Internet access levels for the pupils in their subject or age group, communicating those expectations and setting the appropriate internet access before pupils are allowed to access the Internet. In order to maintain a high level of safeguarding and security, procedures are in place to ensure that everyone with access to the internet uses the internet safely and responsibly.

10. Monitoring and Filtering

10.1 Nicholas Postgate Catholic Academy Trust monitor the use of all ICT Systems including but not limited to the internet, email activity, printing, and application usage on all Trust devices. Internet access is logged and

may be viewed by the IT Staff, senior leaders if requested, and the Police if the need to do so arises.

10.2 Nicholas Postgate Catholic Academy Trust currently employs both Web and Email filtering software to filter/limit access to sites on the Internet and for the scanning of browsers and email for virus protection and key word detection, as an additional safeguarding precaution.

11. Email System Specifics

11.1 **Your Email Account** - All users have access to a NPCAT "professional" email account. This account is provided as part of the Google Suite for Education System controlled, logged and monitored through individual user account access.

11.2 The email system is protected by Google Spam, Virus and profanity filters that provide a high level of filtering,

11.3 The NPCAT IT Team retains admin controls for the issuing and controlling of account availability. The NPCAT IT Team do not have content access to any mailboxes, unless specifically granted by the user or upon an investigation request by a Senior Leader, Headteacher, COO or CEO.

11.4 In order to maintain a high level of safeguarding and security, accompanying procedures are in place to ensure that everyone with access to the email system uses it safely and responsibly.

12. Visitor Network Access

12.1 Visitors are prohibited from connecting any device to the Academy Trust Network. A segregated guest wireless network is provided for visitor access to the Internet if required. The same monitoring policy applies to the guest Wi-Fi.

12.2 Only staff are permitted limited remote access to the Nicholas Postgate Catholic Academy Trust network and server systems. Any individual or company requiring remote access will need to have a valid reason which needs to be approved by the Head of ICT before access is granted.

13. Failure to Comply

13.1 Violations of this policy will be treated like other allegations of inappropriate behaviour at Nicholas Postgate Catholic Academy Trust. Allegations of misconduct will be dealt with according to current policies & procedures.

13.2 We encourage you to use your Email, Internet access, computer account and all other ICT services responsibly. Should you have any questions regarding this Acceptable Use Policy or its associated procedures, please contact the Head of ICT.

14. Legislation

- Computer misuse act 1990 (2022 update)
- Data protection act 2018

15. Related Policies / Procedures

- NPCAT - ICT Systems Acceptable Use Procedure - Employees, Governors & Visitors
- NPCAT – Safeguarding and Child Protection Policy
- NPCAT – Code of Conduct for Governors of a Local Governing Body
- NPCAT – Code of Conduct for Staff
- NPCAT – Confidential Reporting (Whistleblowing) Policy
- NPCAT – Disciplinary Policy
- NPCAT – General Data Protection Regulations (GDPR) Policy
- NPCAT – Managing Allegations of Abuse against Staff Policy
- NPCAT – Media Engagement Policy
- NPCAT – Social Media Policy
- NPCAT – Remote Learning Policy (Online Education)

16. Supporting Information

16.1 The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk

or can visit https://www.saferinternet.org.uk/our-helplines for more information.

16.2 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/

16.3 DfE Guidance – "Keeping Children Safe in Education"

16.4 CES Diocesan Protocols for academies within the trusteeship of the Diocese of Middlesbrough – Section 12 - "Protocol on Safeguarding"

17. Contacts

For advice on the content of this policy, please contact:

Mr Dan Jackson
Head of ICT
Nicholas Postgate Catholic Academy Trust
Tel: 01642 529200
Email: jackson.d@npcat.org.uk

Mr Jim Farquhar
Chief Operating Officer
Nicholas Postgate Catholic Academy Trust
Tel: 01642 529200
Email: farquhar.j@npcat.org.uk