



St Antony's
Roman Catholic School

ASPIRE | BELIEVE | ACHIEVE

General Terms & Conditions for the use of Computer Systems



Bradfield Road, Urmston, Manchester M41 9PD

Tel: 0161 911 8001 Email: stantonysdmin@trafford.gov.uk Website: st-antony.com

Headteacher: Mrs F Wright

St Antony's Roman Catholic School

Pupil Acceptable Use Policy

The use of the latest technology is actively encouraged at St Antony's Catholic College. With this comes a responsibility to protect pupils and the school from abuse of the system.

All pupils, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices (such as mobile phones, smart watches, iPod touches and iPads) within the school, irrespective of who owns the device.

Pupils are expected to behave responsibly on the school computer network and with the ICT equipment, as they would in classrooms and in other areas of the school.

1) Access

As a pupil at St Antony's Catholic College, I have access to the following ICT facilities:

- 1.1 Computer devices throughout the school site
- 1.2 A secure username and password for logging into school computer systems
- 1.3 An accredited, filtered Internet connection from any computer in school or wi-fi connected device
- 1.4 Personal user space on the school network
- 1.5 Personal Google Drive with unlimited storage.
- 1.6 A personal @st-antony's.com email account, via Google Apps for Education, with unlimited storage.
- 1.7 Access to network printers.
- 1.8 Access to resources such as desktop PCs, microcomputers, mobile devices and peripherals.
- 1.9 Access to online resources:
 - i. Google Apps for Education including Google Docs, Slides and Sheets
 - ii. Google Classroom as a VLE and class forum

2) E-safety

- 2.1 I will ensure that I am aware of e-safety issues affecting young people. I will visit www.ThinkuKnow.co.uk and ensure that I have read the guidance provided.
- 2.2 I will only email people I know or that my teacher has approved
- 2.3 The messages I send, or information I upload, will always be polite and sensible
- 2.4 When I use internet sites, I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends unless my teacher has given permission
- 2.5 I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room unless my parent or guardian has given me permission and I take a responsible adult with me.

- 2.6 If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a member of staff.
- 2.7 If I access inappropriate material by accident (eg on a website) I will tell a member of staff.
- 2.8 I will always be myself and will not pretend to be anyone or anything that I am not on the internet.
- 2.9 I will not use email or any communication technology to bully or harass others and I will report instances of online bullying to a member of staff
- 2.10 I understand that if someone makes me an offer via email or the internet that seems too good to be true, it probably is.
- 2.11 If I am in doubt I will ask a teacher or another member of staff.

3) Computer security

- 3.1 I will keep my password secure (secret) and will not give it to anybody else to use
- 3.2 I will log off whenever I finish using a school computer
- 3.3 If I think someone else has my logon details I will report it to a member of staff
- 3.4 I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (eg printers and projectors) and their cabling
- 3.5 I will tell a teacher if I notice that ICT equipment or software is damaged or not working correctly
- 3.6 I will not try to bypass security features or systems in place on the network or try to access anyone else's user account (hacking).
- 3.7 If I find that I do have access to an area that I know I should not have access to, I will inform a member of staff immediately.
- 3.8 I will not open an attachment, or download a file unless I have permission or I know and trust the person who has sent it
- 3.9 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files
- 3.10 I will never attempt to install software on school computers or mobile devices myself
- 3.11 I will not attempt to download software from the internet onto school computers
- 3.12 I will not knowingly install spyware or any sort of hacking software or device.

4) Inappropriate Behaviour

- 4.1 I will not store, download or distribute music, video or image files on my personal user space unless they are appropriately licensed media files (eg Creative Commons licensed files) that I need for school
- 4.2 I will not use indecent, obscene, offensive or threatening language and I will not access material of this kind.
- 4.3 I will not engage in personal, prejudicial or discriminatory attacks
- 4.4 I will not knowingly or recklessly send or post defamatory or malicious information about a person or about school
- 4.5 I will not post or send private information about another person
- 4.6 I understand that bullying, manipulation or exploitation of another person either by email, online or via texts will be treated with the highest severity and possible involvement of the school's designated Child Protection Officer, Mr Speake or Mrs Kelly.
- 4.7 I will not attempt to use proxy sites on the internet
- 4.8 I will not take a photo or video of another pupil or member of staff without their permission

5) Monitoring

- 5.1 I understand that all files and emails on the school computer system are the property of the school. As such, system administrators and staff have the right to access them if required and understand that the content of my Google Drive/OneDrive and school e-mail account is monitored, as are all e-mails that are sent or received, for offensive, inappropriate content, language, phrases and images.
- 5.2 I will not assume that any email sent on the internet is secure.
- 5.3 I understand that all network access, web browsing and emails on the school system and laptops are logged and may be routinely monitored on any computer screen without the pupil's knowledge.
- 5.4 I understand that if I am suspected of breaking this policy, my own personal laptop, storage device or mobile device can be searched by staff with the permission of my parents or carers.
- 5.5 I understand that the school reserves the right to randomly search the internet for inappropriate material posted by pupils and to act upon it.

6) Best practice

- 6.1 I will only print out work that I need as a paper copy – where possible I will use school systems such as email and Google Apps for Education/Microsoft Teams to share information electronically.
- 6.2 I will save, organise my files in a sensible manner work and tidy my user space regularly.
- 6.3 I will observe health and safety guidelines when using computer equipment
- 6.4 I will be considerate and polite to other users

7) Social Networking

- 7.1 I will not load photos or videos of another pupil to website or social networking sites without their permission
- 7.2 I will not load photos or videos of a member of staff to websites or social networking sites
- 7.3 I will never create a bogus social networking account or site that is associated with a member of staff, pupils or the school.
- 7.4 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, pupils or the school, I will inform a member of staff straight away.
- 7.5 I recognise that as an organisation, we do not use social networking sites to communicate with pupils, staff and parents (with the exception of our official Facebook and Twitter accounts).

8) Sanctions

- 8.1 If my actions cause damage to computer equipment, I will be charged for the cost of repairing items broken or damaged through carelessness or vandalism
- 8.2 I may also be charged for the cost of correcting problems caused by hacking or tampering.
- 8.3 I understand that sanctions will vary depending on the severity of the offence, from a warning or withdrawal of internet use to suspension or exclusion. Any breach of the law may lead to the involvement of the Child Protection Officer and the Police.

Useful Websites

Online Safety Helpline - www.swgfl.org.uk/helpline

Free Internet Safety Tips - www.ikeepsafe.org/Free-tips

Kidsmart - www.kidsmart.org.uk

Thinkuknow - <https://www.thinkuknow.co.uk/>

CBBC Stay Safe - www.bbc.co.uk/cbbc/curations/stay-safe

Childnet - www.childnet.com

UK Safer Internet Centre - <https://www.saferinternet.org.uk/>

Keep Children Safe Online - <https://www.internetmatters.org>

E safety tips - www.bullying.co.uk/internetsafety

Online safety | NSPCC - <https://www.nspcc.org.uk>

Pupil Development, Behaviour and Welfare

Assistant Headteacher

Mr Speake – K.Speake@st-antonys.com

Head of Years

Year 7 – Mrs Adderley – L.Adderley@st-antonys.com

Year 8 - Mr Parker-Smith – G.Parker-Smith@st-antonys.com

Year 9 – Mrs Edge – J.Edge@st-antonys.com

Key Stage 4 – Mrs Doherty – E.Doherty@st-antonys.com

Head of Computing

Mr Fearn – m.fearn@st-antonys.com

**Please
cut and
return**

Please cut and return to Mr Fearn (Head of Computing)

Student Signature

I agree to abide by the St Antony's Roman Catholic School Acceptable Use Policy.

Signature Date

Student Full Name (printed) Form

Authorised Signature (Parent / Guardian)

I have read this Acceptable Use Policy and explained the terms of this agreement to my son / daughter.

Parent/Guardian Signature Date

Full Name (printed)