PRIORY SCHOOL
EDGBASTON

ACCEPTABLE USE OF IT

(STATUTORY)

Trustee Committee:	Risk & Compliance	
Date Approved:	1st October 2025	
Next of Review:	October 2027	
Member of Staff Responsible:	L Gough IT Manager	
Trustee Overseer:	Mrs S Watts Rai	
Intended Audience:	Options: Employees, Volunteers, Parents, Pupils and Visitors	
Relevance:	Whole School	Yes
	Early Years	Yes
	Preparatory	Yes
	Seniors	Yes
Access:	Website	Yes
	Internal	No
	Restricted	No

Our Mission Statement

Priory School is a thriving, co-educational independent school founded upon a rich Catholic heritage which welcomes those from all faiths and none.

In partnership with parents and guardians we provide a nurturing, family-based ethos, alongside high-standards of teaching and learning, enabling all pupils to achieve their potential.

We embrace diversity and interfaith understanding alongside awareness of environmental and global issues, in response to the needs of our time.

The Governors and staff at Priory School are committed to providing a fully accessible environment which values and includes all pupils, staff, parents and visitors, regardless of their education, physical, sensory, social, spiritual, emotional or cultural needs.

The Governors, staff and pupils are committed to the safeguarding and welfare of pupils and staff.

To meet the needs of our school community, all our policies, including this policy, can be made available on different formats such as different font sizes or styles, colour, or alternate languages.

The Governing Council understands it has responsibility for ensuring the effective oversight of this policy and will assess, evaluate and review as necessary.

ACCEPTABLE USE OF IT

This acceptable usage policy provides guidance to all pupils on what is an appropriate use of ICT within Priory School. It supplements any legislation around ICT use such as

Data Protection Act (1998)

Computer Misuse Act (1990)

The Online Safety Act (2023)

Copyright, Designs and Patent Act (1998)

Health and Safety (Display Screen Equipment) Regulations 1992 (amended 2002) and government guidelines and initiatives such as the Child Exploitation and Online Protection Body (CEOP).

1. Pupils

Pupils are responsible for good behaviour when using ICT just as they are in a classroom or a school corridor. General school rules apply.

The school has made every effort to provide a safe, educational environment. ICT is provided for pupils to conduct research and communicate with others. Remember that access is a privilege, not a right, and that access requires responsibility.

ICT resources are finite. Downloading large files or accessing certain internet sites may mean other people are denied its use. For this reason certain actions may be restricted.

Individual users of ICT are responsible for their behaviour and communications over the network. At Priory School we expect that users will comply with school standards and will honour the agreements they have been accepted when logging on to the system.

Data on the school network may not be encrypted and so the system should not be used for confidential, sensitive information or anything not related to education at Priory School. For confidential or sensitive matters, specific secure systems are provided. The IT Manager, can view all files, and all data is monitored. The availability of internet services is filtered and controlled by the school, no attempt should be made to bypass these restrictions.

During school hours the staff of Priory School bear responsibility for ensuring the appropriate use of internet services and teachers will guide pupils to the required services for schoolwork. Anything deemed not educational or not age appropriate will be blocked. The school suggests that parents take appropriate measures to ensure this safety and guidance extends into their homes for the pupils.

Here are some examples of what the school does not permit:

1. Sending or displaying inappropriate material.

2. Logging on to other people's accounts, even with their permission.

3. Damaging school devices such as computers, computer systems or computer networks.

4. Violating copyright laws.

5. Downloading files without permission.

6. Use of Chat Rooms.

7. Sending anonymous messages or chain letters.

8. Use of ICT systems for private reasons, without the headteacher's permission.

9. Use of ICT systems for financial gain, gambling, political purposes or advertising.

2. Wireless Networks

Priory School provides access to a filtered, secure wireless network within the site. Pupils may, at the school's discretion, connect to this network using school owned devices that are provided specifically for educational purposes. Users connecting to this network are making use of Priory School's services (networking, internet access etc) and are subject to the same conditions and monitoring as those in ICT rooms.

The school accepts no responsibility for loss, damage or modification to personal equipment used to connect to the network.

3. Sanctions

1. Breaking any of the rules within this document will result in a temporary or permanent ban on ICT use.

2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

3. When applicable, police or local authorities may be involved with more serious offences.

4. Data

Data must be kept in accordance with the Data Protection Act, this also includes data stored on personal laptops, CDs and DVDs, USB sticks and external hard drives. Nobody is at liberty to disclose data to another person that can be considered sensitive and inappropriate to share. An example may be addresses, telephone numbers, e-mail addresses or any item of data that could be considered personal or used to identify and individual. All users of the network are responsible for the day to day management of their data stored on the school network, all should familiarise themselves with storage limits and ensure that unwanted and out of date materiel is deleted on a regular basis. Pupils storing data such as coursework on personal devices and external drives should ensure this is backed up on to the school network.

Any data stored on school systems is considered property of the school and as such, is regularly backed up, access controlled and can be reviewed by the IT Manager when/if required. School systems should not be used for anything personal and by doing so you agree that the school has full control over any data stored.

Data Protection Act (1998):

- Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection.

5. General Computer Use

In general, use of school owned ICT equipment (such as computers, tablets, phones, printers, and print centres), email and the internet within the school should primarily be to enhance teaching and learning.

Priority for computer usage should always be given to the core teaching and learning functions of the school.

6. Personally owned equipment

Pupils and parents must be aware of the risks of bringing valuable items into school and the school does not permit the use of personally owned devices unless a specific exception has been made in writing from the Headteacher.

The school will not be liable for loss or damage to any personally owned device. ICT are not responsible for supporting or repairing any personally owned device.

Using the school network for outside business purposes or personal gain is not permitted.

7. Pupil Accounts

Pupil accounts are allocated when joining the school and pupils are responsible for maintaining their own account, files and sign in credentials.

Passwords must be kept secure and changed regularly (at least once every 180 days).

Pupils must not write their password down or disclose it to anyone.

Pupils must not allow anyone else to use their account and should not use anyone else's account.

Pupils must log off or lock their account when away from a machine and must never leave their account logged in and unattended.

8. Hardware and Software

Everybody has a responsibility towards the care and safe keeping of all ICT equipment.

Portable equipment such as laptops and data storage media such as data sticks and CDs must be kept securely locked away when not in use.

Keep all liquids and food away from ICT equipment and be aware of the health and safety hazards relating to electrical equipment. No food or drink is to be permitted in the ICT rooms.

9. Copyright

Under UK copyright law, all students and staff must respect the intellectual property rights of others when using digital resources. Copyright protects original works such as text, images, music, and software, and using these materials without proper permission or licensing may constitute infringement. Within the school environment, copying, downloading, or distributing copyrighted content—unless covered by educational exceptions or appropriate licences—is strictly prohibited. Users must ensure that any content used for teaching, learning, or personal projects complies with copyright regulations, including fair dealing provisions for non-commercial educational use. Breaches of copyright law may result in disciplinary action and legal consequences.

10. Reporting Faults

Pupils should report all faults on school owned equipment to a member of staff who will then contact then ICT departed. This should be done at the earliest convenience of the member of staff it is reported to. Under no circumstances should a pupil attempt to repair ICT equipment themselves.

Please be aware that any old/broken school ICT equipment to be disposed of must be done through ICT as disposal of electrical equipment is subject to UK government regulations.

11. Email

All pupils are provided with a @prioryschool.net email account subject to parent/guardian approval.

Pupils are responsible for day to day management of their own emails, being aware of the data storage limits, ensuring appropriate usage and regularly checking for information from teachers. Pupils are to be aware that email is treated as data and therefore is subject to guidelines of the Data Protection Act.

Limitations are placed on pupil's email accounts to prevent sending emails to external addresses, this ensures that pupils can only use the school email system for communication within the school.

12. Internet Usage

All use of the internet within school hours should be primarily to enhance teaching and learning.

It is understood that pupils may wish to use the internet for personal reasons. This is permitted as long as it does not interfere with academic activities and does not conflict with other aspects of this acceptable use policy.

Pupils are not permitted to use the internet for any illegal activity; this includes accessing sites meant for adults of 18 years or older such as pornographic or gambling sites.

Pupils must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material.

Use of the school internet and network for the conducting of private business or personal gain is not permitted. The downloading of any unlicensed material such as music, video, TV programs, games, and PDF files is illegal and therefore not permitted.

13. Social Networking Sites

Access to social networking sites such as Facebook, X, Instagram, TikTok and other social networking sites is blocked for pupils and restricted to marketing staff.

It is important that young people understand the risks associated with using social networking sites, it is also important that they know how to stay safe in this environment and how to avoid making themselves vulnerable to a range of issues including identity theft, bullying, harassment, grooming and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment due to an inappropriate personal profile or inclusion on another's profile.

The Child Exploitation and Online Protection body (CEOP) provides some useful guidelines and advice for teachers, parents and children.

CEOP Education is the CEOP Centre's online safety centre, providing advice and tips for pupils, adults and professionals of all ages.

14. Bullying

The school will not tolerate any form of bullying including electronic or online bullying.

The misuse of email systems or the internet for harassing people, such as by sending unpleasant or aggressive messages ('cyber bullying') is on the increase. The proliferation of social networking websites such as X, Instagram, Reddit, Snapchat, and Facebook has made it easier for people to stay in touch with each other but is also being used as a medium to enable harassing and bullying. The school reserves the right to monitor all internet and email activity within the bounds of current legislation in order to keep the internet safe for all at Priory School and to protect from online bullies. It is a condition of this policy that all users of our network accept that internet activity is monitored as well as filtered.

Any instances of bullying will be taken very seriously. As with any other form, cyber or online bullying (involving the use of personal computers, mobile phones etc.) will be investigated fully and will result in appropriate disciplinary action.

15. Pornography & other inappropriate material

Nobody is permitted to access or save any form of pornography or offensive, obscene, violent, dangerous or inflammatory material onto any school device, under any circumstances.

16. Online Safety Act (2023)

In accordance with the Online Safety Act 2023, schools have a vital role in safeguarding pupils from harmful online content and promoting responsible digital behaviour. While the Act places legal duties on tech companies to enforce age restrictions, remove illegal material, and mitigate risks to children, it does not replace the school's existing safeguarding responsibilities. Schools must continue to educate students about online risks, including misinformation, grooming, and inappropriate content, and ensure pupils know how to report concerns. Curriculum planning should incorporate age-appropriate online safety education, teaching

students how to critically evaluate online information, recognise manipulative techniques, and understand the impact of their digital footprint.

17. Hacking

Any type of hacking (defined as attempt to gain access to folders, databases, or other material on the network to which one is not entitled) is considered to be an extremely serious offence.

To comply with the Computer Misuse Act 1990 any pupil who engages in hacking or is found with hacking software/paraphernalia on their computer or network account is liable to face suitable sanctions or potential referral to outside agencies such as the police.

Likewise, physical interference with another user's device or school owned computer will not be tolerated.

The Computer Misuse Act 1990 makes it illegal to:

- Gain unauthorised access to a computer's software or data (hacking), including the illegal copying of programs
- Gain unauthorised access to a computer's data for blackmail purposes
- Gain unauthorised access to a computer's data with the intention of altering or deleting it, including planting viruses
- Copy programs illegally (software piracy).

Staff – in the first instance please refer to the Staff Code of Conduct Document.