PRIORY SCHOOL

Acceptable Use Policy (ICT)

Reviewed by: Julie Evans (Headteacher)	**Autumn 2023**
Next Review Date:	**Autumn 2024**

1. Introduction

1.1. This policy is designed to enable the acceptable use of Priory Schools ICT systems and equipment for all staff and governors.

1.2. Priory School provides a range of ICT resources, which are available to staff, students and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed within this policy.

1.3. This policy aims to:

1.3.1. Promote the professional, ethical, lawful and productive use of Priory School's ICT systems and infrastructure.

1.3.2. Define and identify unacceptable use of the school's ICT systems and external systems.

1.3.3. Educate users about their data security responsibilities.

1.3.4. Describe why monitoring of the ICT systems may take place.

1.3.5. Define and identify unacceptable use of social networking sites and school devices.

1.3.6. Specify the consequences of non-compliance.

1.4. This policy applies to staff members and governors, and all users of Priory School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement, which is attached to this policy. Breach of this policy may result in disciplinary action.

1.5. The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

1.6. If you are in doubt and require clarification on any part of this document, please speak to Robert Marston, ICT & MIS Manager.

2. Context

2.1. Priory School is a maintained community special school for students aged 11-19 with severe learning difficulties and / or disabilities, many of whom have an additional diagnosis of Autism.

2.2. All students have an Education, Health and Care Plan or are in the process of transferring to one.

2.3. Priory School's Vision Statement is "Brilliant Lives", the School's Mission Statement is "To provide a learning community that inspires and empowers individuals to achieve amazing things." Its Core Values are Ambition, Respect, Courage, Pride and Happiness.

2.4. Priory School ensures all students receive a broad and balanced curriculum which supports them to maximise their opportunities and to achieve their aspirations, long-term outcomes in a meaningful, safe and positive way.

2.5. Computing will enrich the lives and experiences of all students by enabling students to participate fully in all their learning opportunities at Priory School, their leisure time and to access their local community and community facilities with greater independence.

2.6. Priory School recognises computing technology can be used to acquire, organise, store, manipulate, interpret, communicate, create, and present information in a variety of ways.

2.7. A high-quality education in Computing will equip our students with the experiences and skills of Computing and ICT that they will use in a rapidly changing technological world.

3. Information & Data Security

3.1. Priory School has dedicated policies relating to Electronic Info and Communications Policy and Information Data Security, both of which should be read in conjunction with this policy. The key requirements for staff are as follows:

3.1.1. All equipment that constitutes the School's ICT systems is the sole property of the School.

3.1.2. No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the ICT & MIS Manager. If software is installed without permission, it may cause extensive damage to the ICT systems security or stability and users could be held personally liable for any costs incurred in rectifying the damage.

3.1.3. The ICT & MIS Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings, computer re-imaging and to ensure compliance with statutory and regulatory responsibilities.

3.1.4. Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

3.1.5. It is a criminal offence to use a computer, iPads or the school network for a purpose not permitted by the school.

3.1.6. Unauthorised individuals must not be allowed to access email/Internet / intranet / network, or other school / LA systems.

3.1.7. All Internet traffic and network usage is recorded and this information can be made available to management on request.

3.1.8. Irresponsible use may result in the loss of network or Internet access for a specified period of time or indefinitely.

3.1.9. Network access must only be made via the user's own authorised account and password, which must not be given to any other person and must not be left on display or easily accessible to others.

3.1.10. All documents, data and emails must be saved, accessed and deleted in accordance with the school's data security, confidentiality and data retentions policies and procedures.

3.1.11. Any confidential data that is transported from one location to another must be protected by device level encryption and comply with school data protection and security protocols. For example, Microsoft Windows Bit Locker is suitable for most common USB Storage Devices and can be setup by the ICT & MIS Manager, if required.

3.1.12. Data protection policy requires that any information seen by any employee with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that an employee maybe required by law to disclose such information to an appropriate authority.

3.1.13. All users must always log off or lock their PC when they have finished working or are leaving the computer unattended for any period of time.

3.1.14. Users are not permitted to connect any personal computers, laptops or other personal devices (such as iPads or USB flash drives) to the schools wired or wireless network without permission from the ICT & MIS Manager.

3.1.15. Students should never be allowed to log on or use any member of staffs network account – these have greater permissions and access to access the school network. Any inappropriate use of or damage to files or network resources will be responsibility of the network account holder concerned.

4. **Safeguarding & E-safety**

4.1. Staff must alert the school's Designated Safeguarding Lead or any deputy if the behaviour of any student may be a cause for concern. Staff will be made aware of the four online safety risk areas: content, contact, conduct and commerce through safeguarding training..

4.2. Staff have a duty to support a whole-school safeguarding approach and to report any behaviour of other staff, which it is believed may be inappropriate or concerning in any way, to the Designated Safeguarding Lead or Headteacher

4.3. A member of staff will actively supervise all student activity, on any internet enabled device (including iPads) at all times.

4.4. No student is to use YouTube or any similar site unsupervised at any time.

4.5. Internet content used in lessons must be checked for suitability before using with students within a learning environment.

4.6. Facebook or any other form of social media is not to be accessed on school premises with the exception of Skype under strict guidance and supervision from the class teacher.

5. School Email

a. All staff and governors are provided with an LGfL StaffMail email account, it is for academic and professional use, no personal use being permitted. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.

b. The sending of emails is subject to the following rules:

i. Language must not include swear words, or be offensive or abusive.

ii. Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.

iii. Sending of attachments, which contain copyright material to which the School does not have distribution rights, is not permitted.

iv. The use of personal email addresses by staff for any official school business is not permitted.

v. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

vi. Any electronic communication which contains any content, which could be subject to data protection legislation (e.g. sensitive or personal information), will only be sent using secure and encrypted email or password protection.

vii. Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.

viii. Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

ix. Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).

x. Staff will be encouraged to develop an appropriate work life balance when responding to email.

xi. Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.

xii. School email addresses and other official contact details will not be used for setting up personal social media accounts.

xiii. When sending any sensitive or confidential information to external contacts/bodies/stakeholders, services such as Egress must be used. Advice on using this services should be sought from the ICT & MIS Manager.

6. Internet Usage

a. Internet access is provided for academic and professional use only.

b. The School's internet connection is heavily filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to ICT & MIS Manager.

c. Staff must not therefore access from the School's system any web page or any files downloaded from the web, which could be regarded as illegal, offensive, in bad taste or immoral or in any manor offensive to others.

d. Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

i. Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;

ii. transmitting a false and/or defamatory statement about any person or organisation;

iii. sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;

iv. transmitting confidential information about the School and any of its staff, students or associated third parties;

v. transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);

vi. downloading or disseminating material in breach of copyright;

vii. engaging in online chat rooms, instant messaging, social networking sites and online gambling;

viii. forwarding electronic chain letters and other materials;

ix. accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

e. Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

f. Where evidence of misuse is found the school may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

g. If necessary, such information may be handed to the police in connection with a criminal investigation.

h. The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

i. Pupils and staff are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

ii. Staff and pupils are not allowed to download files from the Internet or via e-mail programs such as Hotmail onto school computers without permission.

7. **Digital cameras**

a. The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

i. Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.

ii. The use of personal digital cameras in school is not permitted, including those that are integrated into mobile phones.

iii. All photos should be downloaded to the school network only and then removed from the camera/memory card as soon as possible.

8. **File Storage**

a. Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

1.1.1. If information/data has to be transferred it must be saved on an encrypted, password protected, storage device

1.1.2. No school data is to be stored on a home computer, or un-encrypted storage device.

1.1.3. No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email (Egress) or using a school approved and encrypted USB device.

9. Social Media

a. Priory School has a Social Media Policy, which should be read in conjunction with this policy. The key requirements for staff are as follows:

i. Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.

ii. Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.

iii. Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the expressed permission of the Head Teacher.

iv. Members of staff will notify the ICT & MIS Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

v. No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.

vi. No details or opinions relating to any pupil are to be published on any website.

vii. Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.

viii. No opinions regarding another member of staff, which could cause offence, are to be posted.

ix. No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.

x. No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.

xi. Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from the Head Teacher.

xii. Any private social networking sites / blogs etc. that are created or actively contributed to must not be confused with their professional role.

10. Mobile Phones & Personal Devices

a. **Staff Devices**

i. The School accepts that employees will bring their mobile phones to work.

ii. As a general rule, employees are not permitted to make/receive calls/texts during work time. (Excluding break/lunch times)

iii. Staff should ensure that mobile phones are turned off or on silent at all times while on school premises. They should be kept in a locker or secure cupboard, should be on silent and not be left on display. This protects staff from being distracted from their work and from allegations of inappropriate use.

iv. In the event that an employee has a particular reason to have their phone with them, for a specified period of time, they must get prior approval from a member of the SLT. Staff must give the School telephone number to their next of kin in case it is necessary for the staff member to be contacted, in an emergency, during school working hours.

v. The School will ensure that the landline telephone remains connected and available for emergency/urgent contact at all times, except in circumstances beyond control. The School has a digital message recording service which is checked regularly.

vi. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use School provided equipment for this purpose.

vii. Staff should use mobile phones in staff-only allocated areas such as the staff room or PPA Room, or outside the school premises; not in open areas and within view of students regardless of the time of day.

viii. Staff will normally be issued with a school phone where contact with parents, carers or the School may be required, e.g. School journeys.

ix. Using a personal phone. Where possible, all contacts to parents and carers should be made via the school office, or a school mobile. Where this is not possible, in exceptional circumstances staff may need to use a personal phone, in which case the following procedures apply:

1. where contacting parents or carers, they should hide their personal number by inputting 141 in front of the number, for confidentiality purposes;

2. on their return to school, log all calls that have been made on their personal device on CPOMS, recording to whom the call was made and nature of the call, and delete the calls from the personal mobile.

x. In normal circumstances staff are not permitted to use their own mobile phones or devices for contacting students or those connected with the family of the student.

xi. Staff should never store parents' or students' telephone or contact details on their mobile phone, as this allows the possibility of inappropriate contact.

xii. Mobile phones and personally-owned mobile devices brought in to School are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

xiii. Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.

b. Student Mobiles

i. All students' mobile phones and personally-owned devices should be handed to the Class Teacher or responsible staff member, if they are brought into School. They will be kept safely in a locked cupboard in the classroom.

ii. Whilst the School will take every reasonable care, it accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile phones.

iii. It is the responsibility of parents to ensure mobile phones are properly insured. It is recommended that student's phones are security marked and password protected.

iv. Students are not allowed to use personal mobile phones in school or on any school trips, unless agreed by the Head Teacher and Parent/Carer as part of an individual programme.

v. If a member of the staff has any suspicion that a mobile phone brought into school by a student has unsuitable material stored on it, the student will be required to hand over the phone immediately to a member of staff and the parent/carer will be asked to collect it from a member of the SLT.

vi. In circumstances where there is a suspicion that the material on the mobile phone may provide evidence relating to a criminal offence, the phone will be handed over to the School's Designated Safeguarding Lead or any deputy, or the Head Teacher for further investigation and the parent/carer will be asked to collect it from them.

vii. It is not permitted for parents to contact their child via their mobile phone during the School day; all contact must be made via the School office.

viii. A zero-tolerance policy is in place with regards to the use of personal or work-related mobiles or electronic devices by any individual in the following areas;

1. Changing areas
2. Toilets
3. Hygiene Rooms

ix. Failure by staff to comply with the mobile phone policy guidelines could result in disciplinary action.

11. Acceptable use of school iPads

a. Users must ensure the use of protective covers/cases for their iPad at all times. These must not be removed when in use.

b. The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.

c. Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

d. Do not subject the iPad to extreme heat or cold.

e. The iPad is subject to routine monitoring by senior management. Devices must be surrendered immediately upon request by any senior member of staff.

f. Priory School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

g. Priory School is not responsible for the financial or other loss of any personal iPads brought into school.

h. Apps can be requested using the 'App Request Form' which can be found on the Shared Admin drive. Free apps can be purchased and deployed by the ICT Technician. Paid apps must be approved and purchased by the ICT & MIS Manager.

i. If an iPad is damaged in any way, it must be returned and reported to the ICT & MIS Manager as soon as possible. Depending on how the damaged happened; a CPOMS incident or Every ticket should then be logged detailing how the damage occurred.

j. Each class has an allocated iPad along with a charging and data transfer cable, these items are the responsibility of the class teachers.

k. Class iPads are to be returned to the ICT department at the end of each half term or whenever requested. This is to allow them to cleaned, checked for damage and to be updated/serviced as required.

l. Teachers and their class teams are responsible for regularly backing up any data or photos from their allocated iPad.

m. Users are not to change or set their own pin number on any school iPad.

n. Users are not to sign into personal iCloud account on any school iPad.

o. If an iPad is to be taken off the school premises for use on an educational visit, the iPad must be logged out with the school ICT Technician.

    i. The schools Mobile Device Management network now offers a Geo-Fencing feature that is enforced on all school iPads. This means that iPads taken off the school premises will automatically be locked and unusable. This needs to be disabled by the IT Technician or ICT & MIS Manager prior to the iPad leaving the premises.

    ii. Upon return, the iPad must be returned to the IT Technician or ICT & MIS Manager so this feature can be re-enabled.

    iii. If an iPad is taken offsite - do not store or leave unattended in vehicles. The iPad and all data held on it will remain the responsibility of whoever is leading the visit until it is returned to school.

12. Remote Access

a. Microsoft Remote Desktop Services (RDS) is the primary method of gaining Remote Access to the Priory School network. Permission to utilise this RDS is granted by the ICT & MIS Manager or the Head Teacher.

b. The Priory School RDS services is provided by Octavo utilising a Dell SonicWall for additional security.

c. Virtual Private Network (VPN) connections are possible but are strictly controlled and restricted to be used only on school owned devices. This level of access is requires the approval of the Head Teacher.

d. Remote connections are considered direct connections to the Priory School network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this and all other related school policies.

e. Users must ensure that remote access is used for work purposes only.

f. Users with remote access privileges shall ensure that their remote access connection is used explicitly for work use only and used in a manner consistent with their on-site connection to the school network.

g. It is the users responsibility to ensure that their personal computers have adequate and up to date security defences install before attempting to access any remote connection to the school network. Ideally, this should be the school standard software Sophos, which is provided free to all members of staff though the LGFL. Please speak to the ICT & MIS Manager for more details.

h. A home routed and firewalled, internal private network using network address translation (NAT) technology is excepted from this clause provided said network is under the complete control of the user.

i. Users will take full responsibility for any unlawful access, misuse or damages made to the school network, its related assets or any data security breaches.

j. All remote connections are recorded and are available to management on request.

13. Loaning of School ICT Equipment

a. The Head Teacher has agreed that laptops and other school ICT equipment can be loaned to staff while employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time.

b. Staff members to whom equipment has been loaned will be given **a loan form** confirming agreement to the following terms and conditions, as follows:

   i. The Laptop and any accessories provided with it, remains the property of Priory School

   ii. I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop is stolen from an unattended vehicle or a house left unattended for longer than 48 hours, I will be responsible for its replacement.

   iii. I agree to treat the laptop with due care and keep the laptop in good condition, ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop unattended at any time without being stored securely

   iv. I will avoid food and drink near the keyboard/touch pad.

   v. Staff are responsible for ensuring that any laptop or tablet device (IPad) loaned to them is used solely to support their professional responsibilities and that they notify the school of any 'significant personal use' as defined by HM Revenue & Customs.

vi. I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.

vii. I agree to only use software licensed by the school, authorised and provided by the ICT & MIS Manager.

viii. I agree that Anti-Virus and Firewall software is installed and must be updated on a weekly basis. ICT staff from the school will advise on the routines and schedule of this operation.

ix. Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than Priory school ICT staff, attempt to fix suspected hardware/software, or any other faults.

x. I agree that home Internet access is permitted at the discretion of the Head Teacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.

xi. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.

xii. I agree to adhere to School and LA policies regarding the following and will ensure I remain up to date on any changes to the following

- Acceptable Use;
- Data Protection;
- Data Security;
- Social Media
- Safeguarding
- E-Safety
- Health and Safety.

xiii. I agree and understand that from time to time the equipment will need to be returned to the ICT & MIS Manager for updates & patches to be applied, new hardware or software to be installed and general maintenance be carried out.

14. Monitoring of the ICT Systems

a. The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes.

b. If any inappropriate material is found on the school network, it will be deleted without warning and reported to the appropriate line manager or authorities.

c. Monitoring software is installed to ensure that use of the network is regularly checked by the ICT & MIS Manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

d. Other reasons for monitoring the ICT systems include the need to:

i. ensure operational effectiveness of the services provided;
ii. maintain the system security and performance;
iii. prevent a breach of the law, this policy, or any other school policy;
iv. investigate a suspected breach of the law, this policy, or any other school policy.

15. Failure to Comply with the Policy

a. Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

b. Any unauthorised use of the school's ICT systems, cloud or web based ICT systems/services, the internet, e-mail and/or social networking site accounts, which the ICT & MIS Manager or Head Teacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

c. The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.