St Mary's Catholic High School, Leyland

Staff ICT and Electronic Devices Policy

Created: March 2022 Reviewed: Oct 2024 Review by: Oct 2026

1. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The Communications Act 2003
- The Freedom of Information Act 2000
- The Human Rights Act 1998
- Voyeurism (Offences) Act 2019

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- E-safety Policy
- Loaning School Equipment Policy
- Photography Policy
- Data and E-Security Breach Prevention and Management Plan
- Finance Policy

- Records Management Policy

2. Roles and responsibilities

The governing body has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The **headteacher** is responsible for:

- Reviewing and amending this policy with the IT Network Manager and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is carried out daily by the designated equipment lead (DEL). Mr D. Orme
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The IT Network Manager and Assistant Network Manager are responsible for:

- Carrying out checks on internet activity of all user accounts flagged by real-time alerts of the filter software.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher.
- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.
- Ensuring routine security checks are carried out on all school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.

- Disabling user accounts of staff that do not follow the policy, at the request of the headteacher.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the IT facilities and devices, if required.
- Immediately report any breach of personal DPO.

The IT Network Manager is responsible for:

- Ensuring that all school-owned electronic devices have security software installed, to protect sensitive data in cases of loss or theft. Personal devices are not permitted to connect to the school network. They only have access to the guest or visitor network
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the headteacher or IT Network Manager, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to loan school equipment and devices from the IT Network Manager or Business Manager.
- Requesting permission from the IT Network Manager, subject to their approval, before using personally-owned devices during school hours and ensuring these devices are submitted for security checks on a termly basis.
- Ensuring any personally-owned devices that are connected to the school network are encrypted in a manner approved by the IT Network Manager.
- Reporting misuse of IT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The DEL is responsible for the maintenance and day-to-day management of the equipment, as well as the loans process.

The Business Manager is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Overseeing purchase requests for electronic devices.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance Policy.

3. Classifications

School-owned and personally-owned devices or ICT facilities include, but are not limited to, the following:

- Computers/laptops and software
- iPads/Tablets
- School smart phones
- Monitors
- Keyboards
- Mice
- Scanners/visualisers
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Computers
- Photocopying, printing and reproduction equipment
- Recording/playback equipment
- Documents and publications (any type of format)

4. Acceptable use

The school monitors the use of all IT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the GDPR and Data Protection Act 2018.

Any member of staff found to have breached the school's Data Protection Policy or relevant legislation may face disciplinary action.

This policy applies to any computer or other device connected to the school's network and computers.

Staff should always be an example of good practice to pupils, serving as a positive role model in the use of IT and related equipment.

Since IT facilities are also used by pupils, the school has acceptable use agreements for pupils and staff will ensure that pupils comply with these.

Pupils found to have been misusing the IT facilities will be reported to the headteacher.

School-owned electronic devices are not used to access any material which is illegal, inappropriate, or may cause harm or distress to others.
Any illegal, inappropriate or harmful activity is immediately reported to the headteacher.

- Members of staff do not open email attachments from unknown sources.
- Members of staff do not use programmes or software which may allow them to bypass the filtering or security systems.

- All data is stored appropriately in accordance with the school's Data Protection Policy.
- Members of staff only use school-owned electronic devices to take pictures or videos of people who have given their consent.
- School-owned electronic devices are not used to access personal social media accounts.
- Personal electronic devices are not used to communicate with pupils or parents, including via social media.
- Staff representing the school online will express neutral opinions and will not disclose any confidential information or comments regarding the school, or any information that may affect its reputability.
- Staff will ensure the necessary privacy settings are applied to any social networking sites.
- Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.
- Staff will not give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.
- Copyrighted material is not downloaded or distributed.
- School-owned devices may be taken home for work purposes only, once approval has been sought from the IT Network Manager or Business Manager. Remote access to the school network will be given to staff using these devices at home.
- School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.
- While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.
- Private business must not be mixed with official duties, e.g. work email addresses should be reserved strictly for work-based contacts only.
- Use of a school-owned phone for personal use is permitted for necessary calls. A charge may be requested as a result of calls exceeding this time.
- Should staff need to use the telephones for longer than this, authorisation must be sought from the Business Manager. This authorisation must be requested on each occasion. The exception to authorisation is the use of the telephone system to make personal emergency calls, staff should, however, notify the Business Manager after the call.

- Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.
- Family members are not permitted to use school-owned equipment.
- Where permission has been given to use the school equipment for personal reasons, this use should take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.
- Abuse of ICT facilities or devices could result in privileges being removed. Staff should be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, must be reported to the headteacher.
- More details about acceptable use can be found in the staff Technology Acceptable Use Agreement and Device User Agreement.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the internet

- School email is for school business only
- The school email system and internet connection are available for communication and use on matters directly concerned with school business.
- Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.
- All emails should be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.
- Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.
- If any email contains confidential information, the user must ensure that the necessary steps are taken to protect confidentiality.
- The school will be liable for any defamatory information circulated either within the school or to external contacts.
- The school email system and accounts must never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses must not be shared without confirming that they will not be subjected to SPAM or sold on to marketing companies.

- All emails that are sent or received will be retained within the school for a period of **six months** dependent on the information contained. More information can be found in the Records Management Policy. The timeframe will be altered where an inbox becomes full.
- All emails being sent to external recipients will contain the school standard confidentiality notice. That notice is normally configured as a signature by the IT Network Manager and will not be removed.
- Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the IT Network Manager. Access to personal emails must never interfere with work duties.
- Staff linking work email accounts to personal devices, subject to the IT Network Manager's approval, will sign the Device User Agreement and submit their devices for routine security checks on a termly basis.
- The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.
- Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff must never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.
- Purchases for school equipment are only permitted to be made by the Business Manager and a receipt must be obtained, in order to comply with monitoring and accountability. Hard copies of the purchase must be made, for the purchaser and the Finance Assistant. This is in addition to any purchasing arrangement followed according to the school's Finance Policy.
- Any suspicious emails will be recorded in the incident log and will be reported to the IT Network Manager. All incidents will be responded to in accordance with the E-safety Policy.

6. Portable equipment

- All data on school-owned equipment should only be saved on the network as local drives are not backed up.
- Portable school-owned electronic devices should not be left unattended, are kept out of sight and are securely locked away in the staffroom or classroom when they are not in use.
- Portable equipment is transported in its protective case, if supplied.

- Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, only these devices are used.

7. Personal devices

- Staff members will use personal devices in line with the school's Data and E-Security Breach Prevention and Management Plan.
- All personal devices that are used to access the school's online portal, systems or email accounts (e.g. laptops or mobile phones) will be declared and approved by the IT Network Manager before use and submitted for the routine checks outlined in section 14 of this policy.
- Staff using their own devices will sign an agreement stating that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by the IT Network Manager or Assistant Network Manager. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.
- Approved devices must be secured with a password or biometric access control, e.g. fingerprint scanner.
- Members of staff will not contact pupils or parents using their personal devices.
- Personal devices are only used for off-site educational purposes when mutually agreed with the Headteacher/EVC.
- Inappropriate messages are not sent to any member of the school community.
- Permission is sought from the owner of a device before any image or sound recordings are made on their personal device. Consent is also obtained from staff, pupils and other visitors if photographs or recordings are to be taken.
- Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.
- During lesson times, personal devices are kept in a lockable draw/cupboard or kept in personal belongings, out of sight.
-

8. Removable media

Only recommended removable media is used including, but not limited to, the following:

- DVDs

- CDs

- The use of USB removable media is not permitted on the school network. DVDs and CDs containing data, as opposed to videos or music, must be approved first by the IT Network Manager.
- All removable media is securely stored in the data safe in the IT office when not in use.
- Staff will be required to sign removable media devices in and out when they use them.
- Personal and confidential information will not be stored on any removable media.
- The IT Network Manager encrypts all removable media with Microsoft BitLocker.
- Removable media is disposed of securely by the IT Manager.

9. Cloud-based storage

- The school is aware that data held in remote and cloud-based storage is still required to be protected in line with the GDPR and DPA 2018.
- Members of staff ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing messages

- Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of after no more than six months.
- Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.
- If a member of staff is unsure about the correct message storage procedure, help will be sought from the IT Network Manager.
- Employees who feel that they have cause for complaint as a result of any communications on school-owned devices will raise the matter initially with the headteacher, as appropriate. The complaint will then be raised through the grievance procedure.
-

11. Unauthorised use

Staff are not permitted, under any circumstances, to:

- Use the IT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.

- Physically damage IT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the IT facilities without the authorisation of the IT Network Manager. Certain items are asset registered and security marked; their location is recorded by the Business Manager for accountability. Once items are moved after authorisation, staff have a responsibility to notify the SBM of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. The password must be changed when advised by the IT Network Manager. User account passwords must never be disclosed to or by anyone.
- Use the IT facilities at any time to access, download, send, receive, view or display any of the following:
  - Any material that is illegal
  - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
  - Online gambling
  - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
  - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software. without the consent of the IT Network Manager.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.

- Purchase any IT facilities without the consent of the IT Network Manager. This is in addition to any purchasing arrangements followed according to the Finance Policy.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the IT Network Manager. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff must not download or attempt to download any software.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance Policy.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the IT facilities for personal use without the authorisation of the IT Network Manager. This authorisation must be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.
- To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with your responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent

(whether exposed or covered by underwear) – otherwise known as "upskirting".

- Any unauthorised use of email or the internet is likely to result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.
- If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they are encouraged to report this immediately to the Headteacher/DSL.

12. Loaning electronic devices

- School equipment, including electronic devices, will be loaned to staff members in line with the school's Loaning School Equipment Policy.
- Loans will be requested using the Loan Request Form and must give at least three working days' notice prior to the requested loan date.
- Equipment and devices will only be loaned to staff members who have read, signed and returned the terms of use, as set out in the Staff Declaration Form.
- By loaning school equipment and electronic devices, staff members are agreeing to act in accordance with the terms of acceptable use.
- Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.
- The maximum loan period is five working days; however, where required, this can be extended following discussion with the DEL and headteacher.
- If the equipment or device is no longer required, staff members will return the equipment to the DEL as soon as possible, allowing the equipment to be made available to someone else.
- Staff members will be made aware that, at the discretion of the headteacher, late returns may incur a penalty fee.
- Devices allowed for loan will be encrypted and protected to ensure the security of any data they hold.

13. Purchasing

- Funding for electronic devices, predetermined by the governing body, is available each year on request from the IT Network Manager.

- Requests for equipment or electronic devices will be made in writing to the IT Network Manager using the Purchase Request Form.
- Requests must be submitted in sufficient detail for an informed decision to be made. Requests will be responded to within three working days. If sufficient detail is not provided or other conditions specified the request will not be processed.
- Requests made for equipment or electronic devices, which exceed the predetermined amount allocated to require discussion and authorisation by Senior SLT.
- Individual staff members are not permitted to purchase equipment or devices, or process payments for such goods, on the school's behalf.
- The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the school, unless otherwise agreed before with the Business Manager.
- In relation to devices for a specific project, budget holders will provide evidence and a written statement requesting the necessary funds for the equipment required.
- The Business Manager will seek advice from the IT Network Manager and professionals when purchasing equipment.
- All equipment and electronic devices will be sourced from a reputable supplier.
- The Business Manager maintains a Fixed Asset Register, which is used to record and monitor the school's assets. All equipment and electronic devices purchased using school funds will be added to this register.
- When devices are not fit for purpose, staff members may request new equipment. If their request is granted, the old equipment or electronic device must be returned to the IT Network Manager, including any accessories which were originally included with the device. Any old devices will then be disposed of in accordance with ISO: 14001 Environmental and ISO: 27001 Electronic waste recycling and Data destruction standards.

14. Safety and security

- The school's network will be secured using a firewall in line with the Data and E-Security Breach Prevention and Management Plan.

- Filtering of websites, as detailed in the Data and E-Security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked and reported to the IT Network Manager or Assistant Network Manager.
- Approved anti-virus software and malware protection must be used on all approved devices and will be updated automatically when connected to the school network.
- The school will use mail security technology to detect and block any malware transmitted via email – this is monitored in real-time.
- Members of staff must ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, by connecting to the school network on a termly basis.
- Approved personal devices will also be submitted on a termly basis, to the IT Network Manager, so that appropriate security and software updates can be installed to prevent any loss of data. Consent for such access will be obtained before the approval of a device – if consent if refused, the school reserves the right to decline a request to use a personal device.
- Records will be kept detailing the date and time, owner of a device and device type, on which the routine checks have taken place – these will be stored in the IT office.
- Programmes and software are not installed on school-owned electronic devices without permission from the IT Network Manager/Technician.
- Staff are not permitted to remove any software from a school-owned electronic device without permission from the IT Network Manager.
- Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the IT Network Manager/Technician, may be subject to disciplinary measures.
- All devices must be secured by a password or biometric access control.
- Passwords must be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.
- Devices must be configured so that they are automatically locked after being left idle for a set time of no more than five minutes for mobile or other portable devices and 10 minutes for desktop computers or laptops.
- All devices must be encrypted using a method approved by the Network Manager.

- Further security arrangements are outlined in the Data and E-Security Breach Prevention and Management Plan.

15. Loss, theft and damage

For the purpose of this policy, 'damage' is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the IT Network Manager
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

- The school's insurance covers school-owned electronic devices that are damaged or lost, during school hours, if they are being used on the school premises.
- Staff members must use school-owned electronic devices within the parameters of the school's insurance cover - if a school-owned electronic device is damaged or lost outside of school hours or off-site, the member of staff at fault may be responsible for paying damages.
- Any incident which leads to a school-owned electronic device being lost is treated in the same way as damage.
- The IT Network Manager will decide whether a device has been damaged due to the actions described above.
- The IT Network Manager or Assistant Network Manager are contacted if a school-owned electronic device has a technical fault.
- If it is decided that a member of staff is liable for the damage, they are required to pay 20 percent of the total repair or replacement cost.
- A written request for payment is submitted to the member of staff who is liable to pay for damages.
- If the member of staff believes that the request is unfair, they can make an appeal to the headteacher, who makes a final decision within two weeks.
- In cases where the headteacher decides that it is fair to seek payment for damages, the member of staff is required to make the payment within six weeks of receiving the request.

- Payments are made to the Business Manager via the main office, and a receipt is given to the member of staff.

- The school accepts payments made via credit and debit cards, cheques and cash.
- A record of the payment is made and stored in the main office for future reference.
- The Business Manager may accept the payment in instalments.
- If the payment has not been made after six weeks, the fee increases by five percent, and continues for a maximum of six months – at which point formal disciplinary procedures will begin.
- The member of staff is not permitted to access school-owned electronic devices until the payment has been made.
- In cases where a member of staff repeatedly damages school-owned electronic devices, the headteacher may decide to permanently exclude the member of staff from accessing devices.
- If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO must be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies.
- The school is not responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

16. Implementation

- Staff are requested to report any breach of this policy to the headteacher.
- Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.
- Use of the telephone system is logged and monitored.
- Use of the school internet connection is recorded and monitored.
- The **Business Manager** will conduct random checks of asset registered and security marked items.
- The IT staff check server logs on the school network on a daily basis.
- Unsuccessful and successful log-ons are logged on every computer connected to the school's network using Microsoft Azure and Intune.
- Documents sent to the printer are also logged by PaperCut.

- The IT staff can remotely view or interact with any of the computers on the school's network that has Netsupport DNA installed. This may be used on an ad-hoc basis to implement this policy and to assist in resolving IT issues.
- The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.
- The school's database systems are computerised. Unless given permission by the IT Network Manager/Technician, members of staff must not access the system. Failure to adhere to this requirement may result in disciplinary action.
- All users of the school system will be issued with a unique individual password. Staff must not, under any circumstances, disclose this password to any other person.
- Attempting to access school systems using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.
- User accounts are accessible by the headteacher and the IT Network Manager.
- Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.
- Users are required to be familiar with the requirements of the GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.
- Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.
- A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

This page is intentionally left blank

Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.

By signing this form, you are declaring that you have read, understood and agree to the terms of the ICT and Electronic Devices Policy. You should read and sign the declaration below before returning it to the IT Network Manager.

Members of staff are required to re-sign this declaration form if changes are made to the policy.

I have read St Mary's Catholic High School ICT and Electronic Devices Policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- The school reserves the right to monitor my work emails, phone calls, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

Name of staff:	
Job title:	
Department:	
Signed:	
ICT technician signed:	
Headteacher signed:	
Date signed:	

This page is intentionally left blank

St Mary's Catholic High School, Leyland
Royal Avenue, Leyland, PR25 1BS.
Telephone: 01772 421909
Email: head@lsmchs.com
www.lsmchs.com

Device User Agreement – Staff

Employee's Name _____

The school has created this agreement to ensure that the above named person understands their responsibilities when using both school-owned and personal devices, such as mobile phones and tablets, for work purposes whether on or off the school premises.
Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.
Approval from the IT Network Manager must be sought before the use of a personal device can commence. The school reserves the right to access personal devices for the purpose of conducting routine security checks, so that appropriate security and software updates can be installed to prevent any loss of data.

Under this agreement, the school will:

- Provide devices for your sole use while you are a permanent full-time or part-time teacher at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network – remote access to the network will be given to staff using school-owned devices at home.
- Ensure the relevant persons, such as the IT Network Manager or IT Technician, have installed the necessary security measures on any school-owned or personal device before your use – including, but not limited to, the following:
  - Anti-Virus
  - Malware protection
  - User privileges
  - Filtering systems
  - Password protection and encryption
  - Mail security technology

Ensure that all devices undergo the following regular checks and updates by the IT Network Manager/ Technician in line with school policy:

- updates to malware protection
- Termly software updates
- Termly password re-set requirements
- scans in line with specific requirements

- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.
- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage of a school-owned device is a result of your own negligence.
- Ensure that any personal device you access the school network from is appropriate and submitted on a termly basis to the ICT technician, so that appropriate security checks can take place.

Under this agreement, you will:

- Overall use and care of school-owned devices
- Bring the device and charging unit to school at on a regular basis to allow security scans of the device.
- Transport the device safely using the cover and carry case, if necessary, issued with the device.
- Not permit any other individual to use the device without your supervision, unless agreed by the IT Network Manager.
- Take responsibility for any other individual using the device.
- Provide suitable care for the device at all times and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Store devices in a lockable cupboard located in the staffroom or classroom during lesson times.
- Ensure all devices are switched off or set to silent mode during school hours.
- Immediately report any damage or loss of the device to the IT Network Manager.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the IT Network Manager/Technician.
- Be prepared to cover the insurance excess, repair or replacement of the device when the damage or loss has been a result of your own negligence.

- Make arrangements for the return of the device and passcode to the IT Network Manager if your employment ends or if you will be away from the school for more than one week.

Using school-owned and personal devices

- Only use the devices that have been permitted/approved for your use by the headteacher.
- Only use devices for educational purposes.
- Only use apps that are compliant with data protection legislation and from reputable sources.
- Ensure that any personal data is stored in line with data protection legislation.
- Only store sensitive personal data on your device where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device is encrypted and pseudonymised.
- Give permission for the IT staff to erase and wipe school data from your device if it is lost, or when leaving school employment.
- Allow the IT staff to access your personal device (if applicable), to conduct routine security checks to prevent data loss.
- Provide consent and confirm you understand that, if you are using a personal device for work purposes, the IT technician requires access to your device to conduct routine security checks and that there is a potential for your personal information to be seen.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the IT Network Manager.
- Not install any software onto your personal device unless approved by the IT Network Manager. (Staff are not permitted to install software on school-owned devices)
- Ensure your device is protected by anti-virus software installed by the IT Network Manager and that this is checked on a termly basis.
- Not use your device to take images or videos of pupils, staff or parents unless permission has been granted from the headteacher.
- Not store any images or videos of pupils, staff or parents on your device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, only process images or videos of pupils, staff or parents for the activities for which consent has been sought.

- Not use your device to communicate with pupils or parents, unless permission has been sought from the headteacher.
- Not use your device to send any inappropriate messages, images or recordings.
- Ensure that your device does not contain inappropriate or illegal content.
- Only access social media sites as approved by the headteacher on your device, and ensure they are used in accordance with the Technology Acceptable Use Agreement.
- Allow the IT staff to monitor the usage of your device, such as internet access, and understand the consequences if you breach the terms of this agreement.

Insurance cover provides protection from the standard risks whilst a school-owned device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave a school device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the school device being returned to the school and serious breaches may result in disciplinary action.

Please complete this section if you are using a personal device for work purposes.

If you wish to use a personal device for work purposes, you must provide your consent below to allow the ICT technician to access to your device and personal information, to conduct routine security checks and prevent the loss of any data. If you fail to provide this consent, you will no longer be permitted to use your personal device for work purposes including, but not limited to, accessing the online portal, school systems or work email accounts.

I understand the risks posed to my personal information when using a personal device for work purposes and confirm that I will be using a personal device at work. By signing below, I am providing consent for my device to be accessed for security checks and understand how my personal information could be affected.

Signed: Date:

Print name:

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed: Date:

Print name:

Device model and number:

I T Network Manager

Signed: Date:

Print name:

Signed copies to be retained by the employee, IT Network Manager and held on personnel file.

St Mary's Catholic High School, Leyland
Royal Avenue, Leyland, PR25 1BS.
Telephone: 01772 421909
Email: head@lsmchs.com
www.lsmchs.com

Loan Request Form

This form should be completed by staff members when requesting to loan school-owned equipment.

Staff members must detail the specific equipment or device which is requested, as well as provide a reason, and where necessary, evidence, as to why the equipment or device is required.

The completed form should be returned to the IT Network Manager for authorisation.

Name:		**Department:**	
Equipment required:			
Reason:			
First date of loan:		**Return date:**	
Authorised (if rejected, detail why):			
Signed (DEL):			
Job role:		**Date:**	

St Mary's Catholic High School, Leyland
Royal Avenue, Leyland, PR25 1BS.
Telephone: 01772 421909
Email: head@lsmchs.com
www.lsmchs.com

Purchase Request Form

This form should be completed by staff members when requesting for funds for the purchase of equipment or an electronic device.

Before submitting the form, any evidence supporting a purchase request or demonstrating the need for the equipment should be attached.

The completed form should be returned to the IT Network Manager for authorisation.

Name:		**Department:**	
Purchase requested:			
Amount required:			
For use by:			
Reason:			
Supporting evidence:			
How it will benefit pupils:			
Authorised (if rejected, detail why):			
Signed:			
Job role:		**Date:**	