St Edmund Arrowsmith Catholic High School
Prepare the way of the Lord

WHOLE SCHOOL ICT SAFETY POLICY

Rationale:

The Whole School ICT Safety Policy covers the use of ICT systems to support learning, the use of telephones, email, internet and online resources by staff and pupils provided by St Edmund Arrowsmith Catholic High School. This extends to personal equipment brought into school and used during school/working hours.

The purpose of this policy is to ensure:

- Availability – Information is, and continue to be, accessible and usable as normally required.
- Integrity – Information is assured, with regard to version, accuracy and freedom from corruption
- Confidentiality – Information is restricted to the people, and for the purposes intended.
- Protection – Information, networks, equipment, data and activities that might expose the school, staff and pupils to legal action from other parties.

Definition of "Information" – Information within this policy means data, programs, documents, spreadsheets, databases, electronic mail messages (including IM), images and maps of all types regardless of how or where within the school the information is stored or managed.

The policy consists of three sections:

1. Acceptable use of ICT equipment
2. Use of telephones, email and internet by staff
3. Safe use of online resources

This policy is linked to:

- Staff Behaviour and Code of Conduct policy
- Social Media policy for staff
- Anti-Bullying Policy
- Safeguarding Child Protection policy

---

1. Acceptable Use of ICT equipment

Principles

St Edmund Arrowsmith Catholic High School is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure is the responsibility of all staff.

The school encourages staff to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. The school encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets, surface PC's and other portable ICT devices.

As a user of ICT services of the school you have a right to use its computing services; that right places responsibility on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, consequences associate with that breach and you may be in breach of other school regulations.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff are advised of this policy during their induction and of the school's requirement for them to adhere to the conditions therein. Documents are available at all times for reference using the following path: All Staff Group/Staff documentation/policies.

For the purpose of this policy the term "computing services" refers to any ICT resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own ICT to the school's network and the services available are particularly reminded that such use requires compliance to this policy.

Guidelines

Password Security
Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the school.

Issuance and continued use of your User Account is conditional on your compliance with this policy.

User ID's and passwords are not to be shared or revealed to any other party. Those who use another person's credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.

The ICT Network Manager may request your password to enable troubleshooting or repairs to be carried out on your account/device.

General Conditions
In general, use of the school "computing services" should be for your study, research, teaching or the administrative purposes of the school. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- Your use must at all times comply with the law.
- Your use must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised to use.

- You must not use or copy any data or program belonging to others users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Headteacher).
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the ICT Network Manager for installation.
- You must not use any peer-to-peer file sharing software.
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo or other "Messengers", IRC or "chat" unless expressly authorised to do so for work related purposes. Lync is acceptable and is monitored under the internet filtering software.
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the school's facilities, unless specifically related to school activities.
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Headteacher/Governing Body.
- You must not play computer games of any nature whether preinstalled with the operating system or available online.

Data Security
The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to the information, you are reminded of your responsibilities under data protection law.

You should never take a copy of data outside the school's systems. This includes putting sensitive data onto laptops, memory sticks, cds/dvds or into emails. Consideration should be given to the implications of data falling into the wrong hands, and take appropriate steps to mitigate against this.

The school has implemented the following to reduce risk:

- The school has deactivated all ports and no memory sticks are allowed.
- Remote access enables all data to be viewed within the boundaries as in-situ.
- Emails containing sensitive data should be encrypted.

To send a secure email type **confidential** in the email subject. Email encryption is a secure method of transmitting information in a way that only an intended recipient is able to read the contents of an email. This helps to ensure the confidentiality and integrity of the email(s) received by the end-user and protects confidential and identity information from being stolen by unintended recipients. All internal attachments to @arrowsmith.wigan.sch.uk email addresses will not be encrypted.

People receiving external email attachments will have to go through a procedure to view the email. External users experiencing issues opening documents should be directed to the website.

The ICT Network Manager offers a variety of support and information to help you keep data secure. If you are uncertain about any aspect of data security, you must contact him for advice.

Anti-virus and Firewall Security
All personal computers are installed with current versions of virus protection and firewall software. Users are not to alter the configuration of this software unless express permission has been obtained by the ICT Network Manager. The software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files. Users must ensure they are running with adequate and up-to-date anti-virus software at all times. If any users suspect viral infection on their machine, they should inform the ICT Network Manager immediately. If the ICT Network Manager and IT Technicians detect a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

Physical Security
The users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would.
- Keep liquids away from ICT equipment.
- Do not place heavy objects on ICT equipment.
- Do not drop ICT equipment or objects onto it.
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times.
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Staff supervising pupils using ICT equipment should ensure pupils take reasonable care of such equipment.

A separate Staff Tablet Usage agreement should be signed upon issue of a portable device owned by the school, detailing user's responsibilities and conditions of use. (Appendix A)

Remote Access
Remote access to the school's network is possible where this has been granted. Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Monitoring and Logging
Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept no longer than necessary and in line with current data protection guidelines.

Securus/Impero software is used to monitor activity on the network and the details followed are outlined in the E-Safety procedure. (Appendix B)

Such records and information are sometimes required – under law – by external agencies and authorities. The school will comply with such requests when formally submitted.

Breaches of this policy
Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry a possible range of sanctions, consequences and/or penalties. See (Appendix C) for definitions.

In the event a portable computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the school

Process
An investigation will be carried out, in confidence, by SLT under the direction of the Headteacher. That investigation report will be passed to the staff member's Line Manager, to be considered with the school's disciplinary procedure. Each set of disciplinary procedures provide for an appeal stage.

2. Use of telephones, email and internet by staff

Principles
The provisions of this policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or email/the internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of email, telephones and the internet.

The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedures as well at the school's acceptable use and security policies.

This policy has been designed to safeguard the legal rights of members of staff under the terms of both data protection and the Human Rights Act.

Purposes
To provide guidance on inappropriate use of school telephones, email and internet facilities.
To clarify when the school may monitor staff usage of these facilities.

Guidelines

Use of telephones
There will be occasions when employees need to make short, personal telephone calls on school telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of school telephones for private purposes, which are unreasonably excessive or for school purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rate circumstances where there are reasonable grounds to suspect serious misconduct, the school reserves the right to record calls.

Use of Mobile Phones
Mobile phones are for emergency use only and should not be used during the school day, especially during lessons in the sight of pupils. Use of mobile phones during lesson time will be treated as misconduct. However, they may be used before and after school, during break and lunchtime, provided this is out of sight of pupils.

Use of Email
As with telephones it is recognised that employees can use email for personal means in the same manner as that set out for telephones above. Email should be treated like any other form of written communication and, as such, what is normally accepted as unacceptable in a letter or memorandum is equally unacceptable in an email communication.

Employees should be careful that before they open any attachment to a personal email they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory email whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the email to any other address, unless specifically requested to do so by an investigator appointed by the school. Any other use of email for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

Where the school has reasonable grounds to suspect misuse of email in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of email to and from a particular address.

The school also reserves the right to access an employee's email account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the internet
The primary reason for the provision of internet access is for easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate purchases to enhance the ability of its staff to undertake their school role. However it is legitimate for employees to make use of the internet in its various forms in the same way as email above as long as it is not used to view or distribute improper materials such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The school reserves the right to audit the use of the internet from particular personal computers or accounts where it suspects misuse of the facility.

Monitoring the use of telephone, email and the internet
It is not the school's policy, as a matter of routine, to monitor an employee's use of the school's telephone or email service or of the internet via the school's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Headteacher or Governing Body may grant permission for the auditing of an employee's telephone calls, email or the internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operation purposes, under the direction of the Headteacher. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Headteacher/Governing Body or their delegated representative to enable advice be given to the appropriate line manager the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe use of online resources

Principles
This applies wherever access to St Edmund Arrowsmith Catholic High School Management Information Services are provided. This applies to all online resources provided by the school, for example Capita SIMS and SEA Portal. This policy applies whenever information is accessed through St Edmund Arrowsmith MIS, whether the computer is owned by the school or not. The policy applies to all those who make use of St Edmund Arrowsmith's MIS.

Purposes

Security
This policy is intended to minimise security risks. These risks might affect the integrity of St Edmund Arrowsmith Catholic High Schools' data, the authorised MIS user and the individuals to which the MIS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials.
- The wrongful disclosure of private, sensitive and confidential information.
- Exposure of St Edmund Arrowsmith Catholic High School to vicarious liability for information wrongfully disclosed by authorised users.

Data Access
This Policy aims to ensure all relevant aspects of the General Data protection Regulation (2019) and Fair Processing Policy are adhered to.

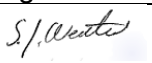
This Policy aims to promote best use of MIS system to further the communication and freedom of information between the school and parents/carers.

Guidelines
St Edmund Arrowsmith Catholic High Schools' online systems are provided for use only by persons who are legally responsible for student(s) currently attending the school.

Access is granted only on condition that the individual formally agrees to the terms of this policy. Unauthorised sharing of student data will be treated as gross misconduct.

Appeal:
Any appeals against this policy will be through the Governor's complaints procedure.

Review:
This Policy will be reviewed every 2 years or earlier if necessary

Date Policy Adopted	**F,P&P Meeting**	Signed:
30 January 2018		
		S J Westhead
		Chair of Governing Body
Policy Reviewed	**16 November 2021**	
	14 November 2023	
Date Policy to be reviewed		
November 2025		

STAFF TABLET USAGE POLICY (APPENDIX A)

Staff have/will be allocated new surface tablets that will eventually replace the computers in their classrooms.

The benefits of this system are anticipated to be:

- A more flexible learning environment where the teacher is not forced to stay at the desk
- Universal access to IT facilities throughout the school
- Less need to log in and set up at the start of lessons regardless of moving rooms
- Ease of access to online systems from home
- Consistent hardware approach (no need for ipads etc.)
- Cheaper infrastructure (no need for projectors + smart boards)
- Remote backup and disk encryption means that work is more secure in every sense
- Control of remote content – school system monitors and filters web usage

Please find below the conditions and responsibilities which must be adhered to at all times to ensure safe and acceptable use of school property:-

USER'S RESPONSIBILITIES

- The tablet 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 tablet.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the tablet screen.
- Do not subject the tablet to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- The tablet is subject to routine monitoring by St Edmund Arrowsmith Catholic High School. Devices must be surrendered immediately upon request by the Headteacher/ ICT Network Manager.
- Users must comply with the password policy set by the administrators.
- Username and passwords should not be shared with anyone, particularly family members and /or friends.
- Due to the financial implications of paid apps from the App Store, we recommend avoiding purchases without first speaking to the ICT Network Manager.
- Users must lock/logoff the device when not present. Preventing data/child protection issues.
- Chargers must remain in school, except if required over the weekend or during a school closure period.

SAFEGUARDING AND MAINTAINING AS AN ACADEMIC TOOL

- Tablet batteries are required to be charged and be ready to use in school. (Charging facilities are available in ICT, however during this period the tablet will remain in the ICT Office)
- The whereabouts of the tablet should be known at all times.
- It is a user's responsibility to keep their tablet safe and secure.
- If a tablet is found unattended, it should be given to ICT Technical Support immediately.

LOST, DAMAGED OR STOLEN TABLET

If the tablet is lost, stolen, or damaged the ICT Network Manager/ Headteacher must be notified immediately.

PROHIBITED USES (NOT EXCLUSIVE)

- Accessing inappropriate materials – All material on the tablet must adhere to the ICT Acceptable Use Policy. Users are prohibited to send, access, upload, download or distribute offensive, threatening, obscene, or sexually explicit materials.
- Illegal activities – Use of the school's internet/ e-mail accounts for financial or commercial gain or for any illegal activity.
- Violating copyrights – Users are prohibited from storing Copyright Music/ Videos on their tablet.
- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos.
- Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the tablet by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- Users should be aware of and abide by the guidelines set out by the school internet policy.
- The tablet must only be used by the individual user; friends/ family members are strictly prohibited from using the device.
- Software should not installed by the user onto the device, it would not be licensed to school and would not be legally covered.
- Installation of software could breach school security and monitoring.

MONITORING/ CONFIGURATIONS

- Tablets are setup using a corporate e-mail address which must, under no circumstances, be removed/ changed.
- Tablets are configured and monitored by ICT Technical Support 24/7 using mobile device management software. It is possible for the ICT Network Manager to obtain data/ usage reports at any time as requested by the Headteacher.
- ICT Technical Support will regularly check tablets for any new updates. During this period tablet users will be notified and ICT Support will require sole access to the device.
- It is possible for ICT Technical Support to remotely view tablets screens using Impero classroom management software
- Tablets are GPS tracked, monitoring the whereabouts of the device and the content accessed.
- Hard Drives are encrypted preventing theft of data in the event of the device being stolen.
- The device uses the School internet filtering when browsing the internet. Logging all websites and content. This happens at ALL times internally and externally.
- The Device connects to the school network at all time. Even when connecting from home.
- Data is backed up nightly and secured on site.
- External use of the device uses a secure connection between the tablet and school. Preventing the device from attack.
- All data must be saved to a School drive and not left on the tablet

I have read and understand the above and agree to use the school device within these guidelines. I understand the tablet remains the property of the school and must be surrendered on termination of my employment or before if requested by the Headteacher.

Staff Name _____

Signed _____

Date _____

E-SAFETY PROCEDURE (APPENDIX B)

1. Securus/Impero Software is to be accessed by the SIMS Officer, with all unviewed violations assessed on a daily basis.
2. The SIMS Officer will view the violations and decide on any necessary action.
3. Viewed violations which need no further action will be archived.
4. Violations judged to need further action will be saved and the violation screen printed.
5. The SIMS Manager and SIMS Officer will jointly decide on the appropriate action relating to the severity of the violation.
6. In minor pupil instances e.g bad language the SIMS Officer will first discuss the situation with the class teacher and they will jointly decide on appropriate action.
7. If necessary, and in cases of very serious violations, the SIMS Officer responsible for monitoring Securus will discuss the matter with the appropriate cluster leader, who will decide on the appropriate action.
8. All violations by members of staff and other non pupils, judged to need further action, will be discussed directly with the cluster leader or Headteacher.
9. The SIMS officer will discuss monitoring issues and current procedures of Securus/Impero each week with the SIMS Manager giving an overall report of the week's incidents.
10. Violations are confidential and will be discussed only with the staff members and pupils directly involved.

Actions resulting from any violations will be actioned following these guidelines:-

An adult violation judged to be serious:

If the material is offensive but not illegal the Headteacher/Cluster Leader should then:-

- Identify the precise details of the material.
- Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure that there is no risk of pupils accessing inappropriate materials in school.
- Remove the equipment to a secure place.
- Take appropriate disciplinary action.
- Inform appropriate Governing Body Committee of the incident. In extreme cases where the material is of an illegal nature.
- Contact the local Police of and follow their advice. If requested to, remove the equipment to a secure place and document what you have done.

A pupil violation judged to be serious:

If the material is offensive but not illegal the Headteacher should then:-

- Identify the precise details of the material.
- Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure that there is no
- Risk of other pupils accessing inappropriate materials in school.
- Remove the equipment to a secure place.
- Take appropriate disciplinary action
- Notify parents of any children involved.
- Inform Governors of the incident.

In extreme cases where the material is of an illegal nature:

- Contact the local Police of High Tech Crime Unit and follow their advice.
- If requested to, remove the equipment to a secure place and document what you have done.

A bullying incident directed at a child or malicious or threatening comments are posted about a pupil or member of staff.

1. Refer to relevant policies
2. Secure and preserve any evidence.
3. Notify parents of any children involved.
4. Inform the police if necessary.
5. Inform the LA e-safety officer if necessary.
6. Support staff

If appropriate send all evidence to CEOP at www.ceop.gov.uk/contactus

DEFINITIONS OF LEVEL OF BREACH (APPENDIX C)

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance.

Examples of this would include:-

- Taking food and/or drink into ICT facilities where they are forbidden
- Sending nuisance (non-offensive) email
- Behaving in a disruptive manner

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties.

Examples of this would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded.

Examples of this would include:

- Repeated moderate breaches.
- Theft, vandalism or wilful damage of/to ICT facilities, services and resources.
- Forging email i.e. masquerading as another person
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using school's computing services and facilities deemed likely to bring the school into disrepute.
- Attempted unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy ICT systems security.
- Attempting to modify, damage or destroy another authorised users data.
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.