ICT Security Policy

(Including Acceptable Use Policy)

Updated September 2024

ICT Security Policy for Jarrow Cross Church of England School

Summary

This policy has been written to ensure consistency throughout the school, and the wider school environment, for all matters relating to confidentiality, integrity and availability of school information and assets.

It has been written by the school, building on the South Tyneside LA exemplar policy. This policy includes our Acceptable Use Policy and is in addition to and operates in conjunction with the E-safety Policy and the Data Protection Policy. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

The objectives of this Policy, which is intended for all school staff, including governors, who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Definitions

"Data Controller" – means the Governing Body of Jarrow Cross Church of England School.

"Encryption" – means the process of transforming Information and Personal Data (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

"ICT Systems" – means any ICT systems operated by Jarrow Cross Church of England School.

"Information" - means any information (including confidential and commercially sensitive information) whether created or held electronically or manually. This includes video and audio recordings and images.

"Personal Data" – means any data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indications of the intentions of the Data Controller or any other person in respect of the individual. Personal Data includes sensitive personal data

as defined by the Data Protection Act 2018.

"Strong Password" – a password which is a minimum of at least 8 characters and is complex using upper and lower case alphabetical characters, numerical characters and punctuation and symbol characters. A Strong password should not contain common dictionary words, the user's date of birth, telephone number or car registration.

Responsibilities:

- Users of the school's ICT Systems, Information and Personal Data must comply with the requirements of the ICT Security Policy.
- The School's Leadership Group shall review this document at least annually.
- Users shall be responsible for notifying the Headteacher of any suspected or actual breach of the ICT security.
- The Headteacher must follow the guidelines for reporting E Safety Incidents issued by the LA if there are any risks to ICT security.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and be made aware of policies and procedures as detailed in the AUP (Acceptable User Policy) to help safeguard ICT Systems, Information and Personal Data.
- Users must only access Information and Personal Data held on school ICT systems if they have been properly authorised to do so. Any doubts about access rights should be notified to the Head Teacher.
- Remote access to Information and Personal Data shall only be provided through a secure link and Users must use a strong password.

Passing on Information

Schools hold Information and Personal Data about children and adults and they process it in a number of ways to improve the quality and standard of their provision. Information and Personal Data is shared electronically from schools to LEAs (pupil transfer data, for example) and examination boards. Schools and LEAs also share Information and Personal Data to a number of statutory bodies (such as QCA), and to contractors who provide other services (content providers, such as ITs Learning, Mathletics or Education City).

Additionally, the Children and Young People's Unit (CYPU) requires local authorities, where necessary, to share information with other local government partners to identify children and young people in danger of social exclusion. Jarrow Cross Church of England School must ensure that measures are in place for the safety and integrity of the Information and Personal Data which is shared and will ensure that it will not be used for any purpose other than that for which it was collected and that it will be securely destroyed when it is no longer needed. All personal information must be transferred using the secure email service – Egress.

Physical Security:

- Do not leave Information or Personal Data on printers, computer monitors or desks whilst away from your desk or computer.

- Do not give out Information or Personal Data unless the recipient is authorised to receive it.

- Do not send Information or Personal Data via e-mail or post without suitable security measures being applied.

- Ensure Personal Data, both paper and electronic, is disposed of properly, e.g. cross shred paper copies and disposed of only in confidential waste bags/bins and ensure all hard discs where Personal Data has been stored or processed are sanitised (forensically wiped or degaussed) before disposal to the DoD standard 5220.22-M/HMG Infosec Standard No 5 with a product such as Kill Disc http://www.killdisk.com/.

- Bulk data transfers must be encrypted to a minimum 128bit/256 AES/3DES and then be transferred via SFTP (Secure File Transfer Protocol) or transferred via HTTPS (HTTP Secure Protocol).

- As far as is reasonably practicable, only authorised Users should be admitted to rooms that contain servers or provide access to Information and Personal Data.

- Server rooms must be kept locked when unattended.

- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

- All school owned ICT equipment and software should be tagged and logged and an inventory maintained and updated a minimum of every 12 months.

- Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.

- Computer monitors should be positioned in such a way that Information and Personal Data being processed cannot be viewed by unauthorised persons.

- Staff must ensure that their laptop access is protected by a strong password.

System Security:

- All Users must have individual, accountable login ID's.

- Passwords for all Users must be a minimum of 8 characters and should be Strong Passwords. Passwords for all Users must be changed a minimum of every 60 calendar days.

- Passwords must be memorised. Passwords must not be written down.

- Individual Login ID's should be locked out after 3 failed login attempts for all Users.

- One time passwords should be created for first login or after resets forcing the User to change the Password at first login.

- Passwords must not be revealed to any other person.

- Passwords must not be obvious or guessable and their complexity should reflect the value and sensitivity of the ICT Systems and the Information and/or Personal Data.

- Passwords must be changed if affected by a suspected or actual breach of security, e.g. when a password may be known by any other person.

- Users must lock workstations when unattended to prevent unauthorised use.

- Weekly backups of Information and Personal Data must be maintained.

- Backups should be regularly tested to ensure they enable data restoration in the event of ICT System failure.

- No User may access the school's ICT Systems, Information or Personal Data, to extract information via a report or by hand, using electronic means, photographic means or paper and then use the data or allow it to be used away from the school premises without the express consent of the Head Teacher. This applies even if the person is authorised to access and view the information in school.

Prohibited Practices:

- Users must not disclose their log on or password details to any other person.

- Users must not disclose Information or Personal Data to any person who is not authorised to have access to that Information or Personal Data.

- Users must not share ICT System access. Allowing others to obtain access using your or another colleague's account password or accessing the ICT Systems via someone else's user login is a disciplinary offence.

- Users must not inappropriately access the systems for personal reasons such as records relating to them, a family member, friend, relative or neighbour.

- Users must not transmit or remove any Personal Data from school premises unless (a) authorised to do so and (b) the Personal Data has been securely encrypted to a minimum of 128bit/256 AES/3DES.

- Users must not publish spreadsheets, databases or other documents containing Personal Data on externally accessible web sites.

- Users must not transfer or permit any transfers of Personal Data to any place outside the European Economic Area, whether by itself or a third party, except with the express prior written authority of the Head Teacher.

This is not an exhaustive list. Any User found to have accessed Information or Personal Data inappropriately may be subject to disciplinary investigation and action.

Termination, change and suspension of Personnel:

Where there is a termination or suspension of school personnel (whether permanent, temporary, agency, casual or contractor) the school must ensure:

- That individual User login ID's and passwords (including any remote access) are disabled immediately upon termination or suspension and that the related active and back up files are reassigned to another or a replacement User.

- That all keys, badges, door passes and other devices used to gain access to premises are retrieved from the departing or suspended User and that the combinations of any locks and/or alarms known to the departing or suspended User are changed.

- That all school-owned hardware (PC's, laptops, smart phones, tablets and media storage devices) software and paperwork are returned to the School prior to the departure of the school personnel.

- That where the school operates a Bring Your Own Device (BYOD) Policy that any school-owned Information, Personal Data or software (including any remote access software) is securely deleted from the personnel's device.

- That where the departing or suspended User had the authority to grant ICT System authorisations to other Users, these other authorisations are immediately revoked.

Where there is a change of role of personnel, the school must:

- Review the access rights of the personnel and adjust those access rights as necessary to suit the new role.

Virus Protection:

- The school must ensure current and up to date anti-virus software is applied to all school ICT systems.

- Laptop users must ensure they update their virus protection at least weekly.

- Any suspected or actual virus infection must be reported immediately to the System Manager or ICT Co-ordinator and that hardware shall not be reconnected to the school network until the infection is removed.

Disposal of Equipment:

Where the School intends to dispose of hardware, by sale or donation, to another organisation or individual, the School must:

- Ensure all hard discs where Information and Personal Data has been stored or processed must be sanitised (forensically wiped or degaussed) before disposal to the DoD standard DoD standard 5220.22-M/HMG Infosec Standard No 5 with a product such as kill Disc http://www.killdisk.com/ The school must ensure that where Information and Personal Data cannot be securely sanitised from any hardware that hardware is physically destroyed.

- Ensure that copies of any files that should be retained are made prior to sanitising and disposing of any piece of hardware.

- Ensure that any software remaining on a PC, laptop or other device being sold or donated for reuse are legitimate and can lawfully be passed on in accordance with any software license conditions.

- Ensure the requirements of the Waste from Electrical and Electronic Equipment Regulations 2006 (WEEE Regulations) are complied with.

Acceptable Use Policy

This policy applies to all staff and visitors at Jarrow Cross C of E Primary School and to those offered access to school resources. This document, which covers Internet and e-mail use, and which does not form part of the contract of employment, may be subject to amendment from time to time.

The Internet system (i.e. Internet and e-mail) is the property of Jarrow Cross C of E Primary School and may be subject to monitoring and access by the School at its discretion. All access to the internet and email system is automatically logged.

Use of the Internet system by school employees is permitted and encouraged where such use is suitable and is in accordance with the goals and objectives of the school. Abuse of such use may lead to disciplinary action being taken.

The Internet system is to be used in a manner that is consistent with the school's ethos, rules and regulations and as part of the normal execution of an employee's job responsibilities.

Generally, the Internet system should be used for business purposes. Reasonable personal use is permitted. However, users may be subject to limitations on their use of such resources.

The distribution of any information through the Internet system may be subject to the scrutiny of the school. The school reserves the right to determine the suitability of this information.

Users shall not:

Visit Internet sites that contain obscene or other objectionable materials. The accessing or downloading of pornographic material is prohibited and is likely to constitute gross misconduct, which may lead to dismissal.

Make or post indecent, demeaning or disruptive remarks, proposals or materials on the Internet system.

Copy, share, forward or display any material, whether internal or external, that is obscene or defamatory or which is intended or likely to harass or intimidate another person.

Disclose any information that is confidential to the school, for example parents' personal details.

Represent personal opinions as those of the school.

Upload, download or otherwise transmit software or any copyrighted materials belonging to parties outside the school or to the school itself.

Download any software or electronic files without implementing virus protection measures that have been approved by the school.

Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

Examine or change another person's files, output, user name or use their password.

The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. The school retains the right to report any illegal violation to the appropriate authorities.

Below are the rules for responsible internet and e-mail use which are published around the school. Additionally an acceptable usage policy window has to be accepted and clicked, by all pupils and staff, before logging on to any PC in the school domain:

Jarrow Cross C of E Primary School

Rules for Responsible Internet and E-Mail Use

At Jarrow Cross access to the computers and to the internet is a privilege. The school PC's and the internet are primarily used for learning. These rules will help us to be fair to others and keep everyone safe. Failure to follow any of these rules will result in your access to the school network being restricted or denied.

- On the school network I will only use my personal username and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will not bring usb devices into school without permission.
- The messages I send will be polite and sensible.
- When using e-mail or the internet, I will not give my full name, home address or phone number, or reveal the personal details of anyone else.
- I will not use Internet chat facilities (such as MSN Messenger), chat rooms or webmail (such as MSN Hotmail, Yahoo!Mail or AOL Mail).
- If I see anything on the internet I am unhappy or uncomfortable with, or if I receive messages I do not like, I will tell a member of staff immediately.
- I know that the school has a filter in place and any inappropriate web searches will be noted.

Updated September 2024