Glynwood Primary School

ICT Security Policy

Contents

Introduction

The use of Information and Communication Technology (ICT) helps Gateshead Council and Glynwood Primary School to provide effective and efficient services and is a vital tool in the work of many employees. To ensure that we obtain the most benefit from ICT, users must understand and comply with their responsibilities in relation to the secure use of ICT resources and the information held within them.

This policy is designed to ensure that all users of the Schools and Council's ICT systems are aware of the security risks that are always present. As such, it is intended to help protect information from all threats whether internal or external, deliberate or accidental.

The adoption of these controls provide a firm indication that the school is taking 'due care' of information which is one of the basic requirements of the Data Protection Act 1998.

Why is this Policy important?

Users who fail to follow the policy risk causing major disruption to School and Council business. Such misuse could result in disciplinary action and/or legal action

What is ICT equipment?

For the purposes of the policy, ICT equipment is defined as being: "Any item of electronic equipment that is capable of storing or transmitting Council information". This includes, but is not limited to, technologies such as:

- Audio recording
- CCTV
- Computers
- E-mail systems
- Fax machines
- Internet access
- Mobile phones
- Scanners
- Telephones
- Mobile radios
- Network equipment and cabling
- Photocopiers
- Photographic equipment
- Printers
- Video conferencing
- Video recording
- Web cameras

Any purchase of ICT equipment or software should be done in consultation with Omnicom Ltd, who provide the school's curriculum network support who will ensure that all items meet relevant standards, are secure and are compatible with existing systems. In addition to this, it is essential that we ensure there is an appropriate data processing contract in place with those, usually software providers, with whom we share pupil/ staff information.

Computer Security

Deliberate unauthorised use of passwords, attempts at unauthorised access to the network and systems, together with the unauthorised alteration of data are all offences under the Computer Misuse Act 1990.

To ensure compliance with the law and Council policy users must:

- not access or attempt to access any files, folders, logs, reports, messages, systems or information without authorisation.
- never let anyone else know their password. Users should inform their line manager if they have reason to believe that someone knows their password.
- not access a computer system using someone else's username and password for any purpose
- not make or attempt to make any changes to the operating system or settings on Council computers.

Personal use of ICT equipment

Personal use of Council computing equipment is allowed, however:

- It must:
  - Occur within a user's own time (i.e. during a lunch break) – please note that there is a separate section covering personal use of the Internet

- It must not:
  - Interfere with the performance of a user's duties
  - Take priority over work responsibilities
  - Result in the school incurring financial loss
  - Bring the school or Council into disrepute
  - Be unlawful or contrary to Council policy or Code of Conduct
  - Be for private business purposes

- School equipment may be used to prepare simple documents or spreadsheets on personal matters such as a letter to a bank or utility

provider. Personal documents should only be stored temporarily on the school's computers whilst they are being prepared and should be deleted from the system after completion.

- Users are allowed to use school equipment to print a limited number of personal documents.
- The printing of personal photographs and images is not allowed.
- All redundant items of computer equipment and storage media, usb sticks, CD's, tapes etc. must be returned to the school office for secure disposal.

Portable Storage Devices

The following list includes examples of portable storage devices but is not limited to:

- Laptop and Notebook PC's
- Handheld equipment – for example, PDA's; 'Blackberries'
- USB memory sticks
- Flash memory cards
- CD's & DVD's
- Portable hard drives

Guidelines for use of Portable Storage Devices

- Portable devices must be stored securely when left unattended. Additionally, devices taken off-site should not be left unattended in public places.
- Portable storage devices must not be used to store sensitive, confidential or personally identifiable information.
- Users must obtain approval from their line manager before creating, moving or copying information, files, folders etc onto a portable storage device.
  A list of files stored on the portable device should be kept in case the device is lost or stolen.
- Information held on portable storage devices is not automatically copied ('backed-up'). To avoid total loss of data, users must ensure that information stored on portable storage devices is 'backed-up' by connecting to the School's network and storing the files on a networked drive.
- Only authorised School employees may use School owned portable equipment.
- Care should be taken to ensure that display screens can not be overlooked.
- Users who are issued with a laptop must ensure that it is logged on to

the network at least once a month to allow the anti virus software to be automatically updated.

- If a portable storage device is lost, stolen or mislaid it must be immediately reported to the Headteacher
- Visitors or contractors who bring their own USB devices into the school (to give a presentation for example) should be supervised at all times whilst the device is connected to School equipment

School Admin network – Housekeeping

- Business data and files should be saved on a shared network drive in accordance with the school's Record Management Policy. This will allow other users to access the information in your absence. The Z:\Drive should not be used to store such data.
- Users must ensure that their file and folder permissions are set appropriately. Please contact Omnicom for advice on how this should be done.
- Users must ensure that sensitive or classified information is not left on view or lying on desks whilst unattended.
- All school computers must be left with a clear screen whilst unattended. Users should 'lock' the screen whenever they leave their desks (using ctrl/alt/delete) even for short periods of time.
  If the computer is to be left unattended for long periods, users should 'log-out'.
- Sensitive or classified information should be cleared from printers, fax machines, copiers, scanners etc immediately.
- Computer printouts and any other documentation containing personal information no longer required must be shredded.
- Computer equipment that is not being used for long periods, overnight and at weekends for example, should be switched off to conserve energy.

Curriculum network – Housekeeping

Software

- All software (including fonts, shareware and freeware) to be used on school computers should be done so in consultation with Omnicom Ltd.
- All computer software must be used in accordance with its licence agreement.
- All software must be catalogued and held centrally by the ICT coordinator as appropriate

Anti Virus Precautions

- All incoming e-mails on the council's admin network are scanned for viruses before they reach a users 'Inbox'. However, because new viruses are created almost daily, it is important that users are cautious at all times. All e-mails, especially those with attachments, could be a risk. If there is any doubt, users must contact the SBM/ ICT coordinator before opening e-mail or attachments
- Files on CDs, DVDs or USB memory sticks are automatically scanned for viruses as they are opened.
- Users who get a virus alert from anywhere other than SBM/ ICT coordinator should inform them.
- Do not forward a virus alert message to anyone else.

Internet Access

The Internet can be a very useful tool for getting information quickly and easily. However, access to the Internet also presents a number of risks to both the School and users. This policy defines what is acceptable, what is not acceptable and what controls must be followed when using Council equipment to access the Internet.

Specific requirements

The following requirements apply to all use of the Internet for School purposes and personal use using School's equipment:

- Users must not intentionally access or attempt to access information or images that are obscene, sexually explicit, racist or defamatory or which depict violent or criminal acts or otherwise represent values that are contrary to school policy
- All access to the Internet must be via a method approved in advance by the headteacher
- Users must not access or attempt to access Internet based file sharing networks, typically used for downloading and sharing music and video files. If you are in any doubt you must seek for advice before attempting to access any website.
- A user who accidentally opens a website showing material that breaches school guidelines must exit the site immediately and report it without undue delay.
- Any user who tries to access a website that is thought to be within School/ Council guidelines but finds that it is blocked should ask for it to be unblocked through the ICT coordinator

Copyright

Much of what appears on the Internet is protected by copyright. This can include images and logos, as well as documents and information. The Copyright, Designs and Patents Act 1988 states that only the owner of the copyright is allowed to copy the information and any copying without permission, including electronic copying, is prohibited.

Spyware

Spyware programs interfere with the normal running of a computer and/or collect and transmit potentially sensitive data without the user's knowledge. These programs are often 'hidden' in 'free' software offered by websites.
Users must not install or attempt to install any software or web browser toolbars.
Users who suspect that their computer may be infected with spyware should contact the ICT Coordinator.

Personal use of the Internet

Personal use of the Internet is allowed however it must not have a negative impact on the School by:

- Being unlawful or contrary to School policy or Code of Conduct
- Bringing the School into disrepute
- Interfering with the performance of a user's duties
- Taking priority over a user's work responsibilities

Personal use - What Users CAN do

- Access browser based personal e-mail systems (for example, log on to webmail to check personal e-mail)
- Browse web pages, (check the latest news, research a hobby, bank online for example)
- Buy goods and services online for personal use where a download to the computer is not required (shop online, book a flight or holiday, use online auction sites for example)
- Print information – a limited amount of personal printing is allowed

Personal use - What Users CANNOT do

- Access Chat Rooms
- Buy music, video etc if it requires a download

- Change settings on school computers
- Create or update a personal website
- Download and / or upload software
- Use a school e-mail address to subscribe to websites accessed for personal use
- Use it for private business purposes
- Use it for gambling

The School uses a number of measures to protect its computers from viruses and spyware etc. However, no guarantee can be given that personal details, bank and / or credit card details are secure. Users who choose to enter personal details or buy online do so at their own risk.

Forums

Internet discussion forums can be an effective and efficient method of sharing information and best practice with peer groups and similar organisations. However, users must be aware that any comments posted on a forum may be visible to anyone in the world with an Internet connection. Users who join an Internet discussion forum must conduct themselves in an honest and professional manner and care must be taken when disclosing information. All views expressed must reflect the views of the School and must be in accordance with the school's Code of Conduct. This applies for both school business use and personal use of the Internet.

Facebook and similar

The school will adhere to the Local Authority's social media abusive comments guidance for school staff.

Monitoring

Business and personal use of the Internet is monitored and usernames, websites visited, dates and times of the visits, and the time spent at each site is recorded.

Where there is reason to suspect misuse, management are able to access detailed reports of this information.

E-mail

Whilst e-mail may often appear to be an informal method of communication users should remember that it has the permanence of written communication,

and as such users must ensure that it meets the same standards as other published documents. You need to think about information security when you send confidential information by email. The consequences of an email containing sensitive information being sent to an unauthorised person could be a civil penalty of up to £500,000 from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information such as a pupil's name in the subject line of an email.

All e-mail and attachments sent and received on School equipment (including personal e-mail) are owned by the School. When using e-mail as a means of communication users should be aware that:

- Advice given by e-mail has the same legal effect as that given in any written format
- All e-mails on the council's citrix system are archived and a copy is retained by the Council for a minimum period of 6 months, including those that have been deleted from mailboxes. Also, you must remember that although you may have deleted your copy of an email, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.
- All e-mails are potentially subject to disclosure under the Freedom of Information Act and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.
- E-mail communications, both internally and externally, can not be guaranteed to be private or secure, nor to arrive at their destination either on time or at all
- E-mails may be produced in court in the same manner as any other Council document
- Once an e-mail has been sent there is no control over who the recipient may then forward it on to, either intentionally or accidentally
- The impersonal nature of e-mail messages can mean that it is easier to cause offence than when speaking and attempts at humour can easily be misinterpreted
- Users must not keep e-mails that are construed as business records in e-mail folders. These e-mails should be saved on a shared drive in accordance with the Council's Records Management Policy.
- All attachments in email should be saved into an appropriate electronic filing system or printed out and placed on paper files

- Where the text of the email adds to the context or value of the attached documents it may be necessary to keep the whole email. The best way to do this and retain information which makes up the audit trail, is to save the email in .msg format or to save the email in an electronic filing system. Where appropriate the email and attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the email in .msg format will.

What NOT to do when using e-mail

When using the School's/ Council's e-mail system any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in e-mail messages.
Additionally, users must not:

- Conduct any business other than that of the School/ Council via e-mail
- Enter into any commitment on behalf of the School unless explicitly authorised to do so. Agreements entered into by email form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.
- Forward chain mail or jokes
- Forward messages unnecessarily
- Generate e-mail in such a way that it appears to have been sent from someone else
- Read, delete, copy or modify the contents of any other user's mailbox without prior authorisation in writing from a Head of Service, unless access has been delegated to that mailbox by the mailbox owner
- Register for automated alerts or subscription services unless there is a valid business reason for doing so
- Send information of a sensitive or confidential nature to a home e-mail account. If an employee needs access to the Council's e-mail system from home they should contact ICT Services who will arrange for secure access to be set up, subject to authorisation by a line manager.
- Send or forward e-mail that could be construed as obscene, sexually explicit, racist, defamatory, abusive, harassing or which describes violent or criminal acts or otherwise represents values or opinions that are contrary to Council policy. Employees who receive

e-mail of this nature should inform their line manager immediately
- Send unsolicited bulk e-mail or Spam
- Use a personal e-mail account for Council business purposes
- Use e-mail to send frivolous messages or gossip

Personal use of e-mail

Personal use of e-mail is allowed, however it must not:

- Be unlawful or contrary to the School's Code of Conduct
- Have a negative impact on the School
- Interfere with the performance of the user's duties
- Result in the School incurring expense
- Take priority over work responsibilities

The rules governing business use of e-mail are also applicable to all personal use of e-mail. Users should create a folder named "Personal" within Outlook. Any sent or received e-mail that is of a personal nature should then be moved into that folder. E-mail in this folder will not normally be accessed by others. However, others may be allowed access as part of an investigation, or on suspicion of inappropriate or excessive use of e-mail by a user. E-mail relating to school business must not be stored in the Personal folder.

Access to a user's mailbox by others

There may be occasions, if a user is away from the office for an extended period for example, when it is necessary for a line manager or a colleague to access e-mail messages in the mailbox of another user. Access to a user's mailbox may also be granted to action:

- Evidence in a criminal investigation
- Evidence in legal proceedings
- Evidence in support of disciplinary action
- Freedom of Information requests
- Subject access requests under the Data Protection Act

Encryption and Digital Signatures

On the admin network, If it is necessary to send or receive information of a personally identifiable or sensitive nature to or from an external recipient it must be encrypted and where applicable, digitally signed. Users should note that password protection of a Word document or Excel spreadsheet is not a secure method of safeguarding data and should not be used to transmit sensitive or confidential data. Please contact ICT Services for advice on encryption and digital signatures.

Spam e-mail

Junk e-mail or Spam is a major problem across the Internet. Although the council's e-mail system blocks tens of thousands of Spam messages every month the large number of such e-mails involved means that some will still get through.

If this happens:

- Do not respond to Spam
- Do not try to unsubscribe from a Spam e-mail – Any response will allow the sender to know that the e-mail address is valid and will probably result in more spam e-mails
- Do not react to false virus reports. These reports tell the user how to take measures against a so-called virus. In reality there is no virus, but following the instructions may damage the computer

Monitoring of e-mail

ICT Services/ Omnicom Ltd make every effort to ensure the privacy of user data, including e-mail messages. Any information obtained by ICT Services/ Omnicom Ltd during the course of systems administration will be treated as confidential and will not be used or disclosed in the normal course of events. Where routine systems management (i.e. technical management of the system to ensure that it is operating correctly) or administration indicates a breach of Council policy or the law, ICT Services/ Omnicom Ltd will bring this information to the attention of the Council/ Headteacher or other relevant authorities.

How long to keep emails?

Email is primarily a communication tool and email applications are not designed for keeping email as a record in a storage area meeting records management storage standards.
Email that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these emails will then correspond with the classes of records according to the schools' disposal of records schedule. These emails may need to be saved into an appropriate electronic filing system or printed out and placed on paper files.

Telephone systems

All outgoing calls from School telephone systems are logged. The log records the date and time of the call, its duration, the extension that was used to make the call and the number called.

When using a School telephone, users should take care that the information being discussed is not overheard by passers-by. Users should also be aware of the importance of checking the identity of all callers requesting personal or otherwise sensitive information.

It is accepted that occasionally users may need to make personal telephone calls whilst at work. However, users should make sure that the facility is not abused and that office telephones are not unduly tied up with personal calls.

- It also applies to incoming as well as outgoing personal calls.
- The amount of work time taken up by personal calls must be kept to a minimum.
- This applies to internal and external personal calls.
- Wherever possible personal calls should take place outside work hours, for example during lunch breaks.

Fax machines

Confidential information can be vulnerable when sent by fax to others. Mail is usually sealed, but faxed documents can be read by anyone who has access to the fax machine. For this reason careful consideration should be given to the positioning of fax machines.

Users should be aware that the responsibility for the fax lies with the person sending, or asking for the fax to be sent.

Voice mail

When used correctly voice mail systems offer a convenient method for callers to leave non-urgent messages when there is no one available to answer the telephone. It is important therefore that users are aware of the following points in order to ensure the system is used securely:

- Do not use simple number sequences for example 0000, 1111, 1234 etc when creating PIN codes.
- PIN codes must be kept confidential. It must not be disclosed to anyone and should be changed regularly

Mobile phones

All access to the Internet, television, video, radio and other media, whether for School/ Council business purposes or personal use, must be via a method approved in advance by the Headteacher. Personal mobile devices should not be used to access school emails or save school related information.

Reprographic Equipment

Cameras

As with any other item of ICT equipment, only cameras procured through School may be connected to the School/ Council network or computers. Personally owned cameras/ mobile phones must not be connected.

Printers, Photocopiers

Care should be taken to ensure that printing is sent to the correct printer to minimise the risk of unauthorised viewing. Users should ensure that sensitive or confidential information is not left unattended on a printer, photocopier.

Incident Reporting and Monitoring

Incident Reporting

Any user who knows of a security incident or suspects someone is misusing the School's computers either deliberately or accidentally must report it to the Headteacher or e-mail Incident Reporting (incidentreporting@gateshead.gov.uk) as quickly as possible. The Headteacher is responsible for ensuring that the incident is recorded and the Council's Incident Reporting Group are informed without undue delay.

The procedure for incident reporting is covered in more detail in the Council's Confidential Reporting Code, which is available on the Intranet.

Monitoring of Activity

The School/ Council reserves the right, consistent with the relevant legislation, to exercise control over ICT resources and to monitor their use to ensure efficient operation, to detect misuse and to supply evidence if required, for use in disciplinary or legal proceedings.

By using School/ Council ICT systems users accept that all use may be monitored.