Greenside Primary School

Information Security Policy

Introduction

This policy is written with reference to the Gateshead Council ICT Security Policy 2009 with adjustments made to reflect the data held and the ICT systems operating within the more specific context of Greenside Primary School, the curriculum server and any stand alone devices. Any member of staff accessing the Administrative Server does so primarily under the conditions of the Gateshead Council ICT Security Policy but also with reference to any further requirements specific to Greenside Primary School outlined in this policy.

Greenside Primary School recognises that Information and Communication Technology (ICT) is an essential tool used to provide effective and efficient services. Information held within ICT systems is a key resource and we have to make sure that it is used appropriately and securely, and Greenside Primary School and the Council are protected against potential security threats. Additionally, we must ensure that any paper based data held in school relating to staff or children is protected and managed effectively.

This policy sets out Greenside Primary School's approach to Information Security. It is intended to help employees to understand the implications of working with ICT and paper based data and their responsibilities in relation to its use.

It is important that we all take our responsibilities seriously, as we want everyone to be able to work with protected information in a safe and secure environment. All employees are responsible for making sure that the policy is put into practice. With the co-operation of everyone, this policy will improve Information Security within Greenside Primary School.

Why is this policy important?

Users who fail to follow the policy risk releasing secure information about pupils or staff and cause a major disruption to school and council business. Such misuse could result in disciplinary action and / or legal action.

Who does this policy apply to?

This policy applies to anyone who has access to Greenside Primary School ICT systems or any additional data relating to pupils and staff at Greenside Primary School, including the following:

- Employees
- Governors
- Employees of partner organisations (e.g. Children Centre, Extended School Cluster)

- Gateshead Council employees (e.g. ICT service staff, RAS employees, auditors)
- Contracted employees (e.g. staff from supply agencies)
- Work placements (e.g. ITT, Teaching Assistant trainees, work experience students)
- Visitors
- Voluntary sector workers
- School-based volunteers
- External auditors / Inspectors

What is ICT equipment and additional data?

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:

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

Users must contact ICT services before procuring any item of ICT equipment or software. ICT service will ensure that all items meet Council standards, are secure and are compatible with existing systems.

For the purposes of the policy additional data relates to any data held which if released without permission would be in breach of the Data Protection Act 1998. This includes but is not limited to:

- Personally identifiable information (e.g. names, addresses, dates of birth, telephone numbers)
- Sensitive or confidential information about a specific person (e.g. assessment data, medical information, involvement with other agencies)

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 the Headteacher 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
- not install, attach, insert, connect, attempt to connect or remove any item of equipment to or from a school laptop computer or the Council or school network without prior authorisation from the Headteacher (who will take advice from ICT services).
- members of staff should not attach their own devices (such as cameras or mobile phones) to school equipment. However, a member of staff may attach their own printer or internet connection device to a school laptop held at home as long as internet security software is up to date on the device.
- obtain permission from the Headteacher and sign out (countersigned by Headteacher or Deputy Headteacher in her absence) before taking and/or using school owned equipment anywhere other than their normal work location.
- ensure that computing equipment, peripheral devices, software to be used for school business purposes are procured primarily via ICT services and where this is not practical or does not provide best value following consultation with ICT services to ensure compatibility and security of equipment.
- be authorised before using school equipment. Provision of a personalised username and password signifies authorisation. In the case of volunteers or visitors, access to the school network should be via a generic password and the date, time and duration of use should be logged in the school office by the member of staff granting access. This member of staff is also responsible for briefing the proposed user on correct protocol for use of equipment.
- members of staff taking school equipment off the premises are responsible for ensuring that no other person (including members of their family) uses this piece of equipment.

Personal Use of School or Council ICT equipment

Personal use of School or Council equipment is allowed, however:

- It must:
    - occur within a user's own time (i.e. before or after directed time or during a lunch break). Please refer to the 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 or Council incurring financial loss
    - bring the school or Council into disrepute
    - be unlawful or contrary to School or Council policies or Code of Conduct
    - be for private business purposes

- School or Council 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 or Council'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. Users must pay for all printing in line with a scale of charges (as detailed on the Council Intranet – please discuss this with office staff)
- The printing of personal photographs and images is not allowed.
- School equipment must not be used for playing games, music, videos etc (personal use only – this does not apply where a member of staff is accessing these with a direct link to pupil learning)
- Personally owned ICT equipment must not be connected to the School or Council network or laptop computers (with the exception of a home printer or internet connection).
- All redundant items of computer equipment and storage media such as floppy discs, CDs, tapes etc must be returned to ICT Services via 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 PCs
- Handheld equipment – for example PDAs, Blackberries
- USB memory sticks
- Flash memory cards
- CDs and DVDs
- Portable hard drives

Guidelines for use of Portable Storage Devices

- Portable devices issued to employees remain the property of Greenside Primary School with the user assuming temporary 'custodianship' of the device.
- All mobile devices must be security marked (asset tag, etched, permanent marker and smart water / UV pen) as soon as they are received into a department or service and then added to the appropriate inventory.
- Records must be maintained detailing the portable device. Provision should be in place for the signing out and return of shared equipment such as cameras or Flip videos. All members of staff issued with laptops or encrypted memory sticks should complete a Portable Storage Device User's Agreement (see Appendix 1).
- Portable devices must be stored securely when left unattended. Additionally, devices taken off-site should not be left unattended in public places, including client's homes.
- If a school owned portable device is lost, stolen or mislaid it must be immediately reported to the Headteacher.
- Portable storage devices must not be used to store sensitive, confidential or personally identifiable information (including photographs) without prior consultation with the Headteacher and if permission is granted then this type of information should only be held on a school issued encrypted memory stick which has been purchased via ICT Services. School laptops are not encrypted and should not be used to store sensitive, confidential or personally identifiable information (including photographs). This type of information should not be stored on employees' personal computers.
- Users must obtain approval from the Headteacher 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 or Council network and storing the files in a networked drive.
- School computer equipment must not be connected to any other computer network.
- Only authorised School employees may use School owned portable equipment.
- Care should be taken that display screens cannot be overlooked when dealing with sensitive information.
- Users who are issued with a laptop should ensure that the virus software is up to date and should refer it to ICT services for an update at the relevant time.
- Visitors or contractors who bring their own USB devices into school (to give a presentation for example) should be supervised at all times whilst the device is connected to school equipment.

Handling Confidential Information

Housekeeping

- Users must ensure that sensitive or classified information is not left on view or lying on desks whilst unattended.
- All paper copies of sensitive or confidential information should be locked away whilst not in use.
- All school computers should be left with a clear screen whilst unattended. 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 print outs and any other documentation no longer required must be disposed of in a controlled and secure way by the person responsible for it (it should not be left sitting on a shredder).
- Computer equipment that is not being used for long periods, overnight and at weekends for example should be switched off to conserve energy.

Sending Confidential Information

It is the responsibility of all employees of the Council to safeguard the security of confidential and / or personal data for which they are responsible or which they access in order to carry out their job. There is also a responsibility to bring to the Headteacher's attention any areas of concern regarding the transfer or transportation of such information.

As a general rule, personal and sensitive data must not be disclosed, transferred or copied to third parties without authorisation from the Headteacher.

Before making information available to anyone else, employees must make sure that they have the authority to disclose it.

Information transported by surface mail must be protected from unauthorised access and environmental damage. External organisations should be requested to use secure post when forwarding confidential information, using tamper-evident packaging when possible.

When using internal mail, confidential information must be placed in clearly identifiable envelopes and must be protected from loss and accidental viewing, using lockable storage equipment where appropriate.

Electronic data physically transported between sites, departments or organisations must be properly packaged and clearly labelled to ensure it is handled correctly and not corrupted by magnetic fields or other environmental damage.

Any breach of security or loss of data must be reported immediately to the Headteacher.

Providing information by telephone

Information must never be given out over the phone or by another verbal means unless it is absolutely clear who it is being given to and that they are entitled to the information and are ready and able to accept it.

Care must be taken to ensure that conversations involving personal, sensitive or confidential information cannot be overheard.

Voicemail messages containing personal information should only be left after due consideration has been given to the security and confidentiality risks involved.

Providing information by Fax

If sending personal information by fax, top sheets must be clearly marked 'Private and Confidential', together with the number of pages being sent and the contact details of the sender.

A time must be agreed with the recipient for the sending of the fax, and confirmation of delivery or non-delivery must be given.

A confirmation sheet should be printed and filed as appropriate. The fax machine should also be checked to ensure that its memory does not retain a record of the transmission.

Providing information by email

Email is not a secure means of communication outside the security of the Council network and must not be used for sending personal or sensitive corporate data.

Even when emailing within the security of the Council network it is important to ensure the name and email address of the recipient is correct and that a suitable subject line is used which does not include personal information.

The sender must also ensure that the recipient is expecting the information and confirm that it has been received successfully.

Software

- All software (including fonts, shareware and freeware) to be used on school computers must be bought and installed through ICT services where possible. If this is not possible then purchasing should be done following discussion with ICT services. Software should not be installed on stand alone equipment without the prior knowledge and permission from the Headteacher.

- All computer software must be used in accordance with its licence agreement
- All software must be catalogued by the ICT co-ordinator

Anti Virus Precautions

- All emails on the Council server are scanned for viruses before they reach a users 'Inbox'. Other email accounts may not be scanned. It is important that users are cautious at all times. All emails, especially those with attachments, could be a risk. If there is any doubt, users must contact the ICT helpdesk before opening email or attachments
- Files on DVDs or USB memory sticks are automatically scanned for viruses as they are opened on the Council Server.
- Users who get a virus alert from anywhere other than ICT Services should inform the ICT helpdesk
- 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 Council and users. This policy defines what is acceptable, what is not acceptable and what controls must be followed when using School or Council equipment to access the Internet.

Specific requirements

The following requirements apply to all use of the Internet both for School / Council purposes and personal use using Council 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 of otherwise to represent values that are contrary to School or Council policy.
- All access to the Internet must be via a method approved in advance by the Headteacher or ICT Services
- 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 contact ICT Services for advice before attempting to access any website.
- Users must not access or attempt to access social networking sites using School or Council equipment.
- A user who accidentally opens a website showing material that breaches Council guidelines must exit the site immediately and report it to the Headteacher followed by a report to ICT Helpdesk without undue delay.
- Any user who tries to access a website via the admin system that is thought to be within Council guidelines but finds that it is blocked should ask for it to be unblocked using the online form on the Intranet.

Purchasing online

Users must not acquire or buy any goods or services for Council business purposes directly from web sites or other Internet sources. Users should first contact Corporate Procurement for confirmation that they are complying with the latest procurement procedures.

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 Helpdesk.

Personal use of the Internet

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

- being unlawful or contrary to School or Council policy or Code of Conduct
- bringing the School or Council into disrepute
- interfering with the performance of a user's duties
- taking priority over a user's work responsibilities

On the Council system, personal use is only allowed between the hours of 12:00midday and 2:00pm, Monday – Friday, and must be done in the employee's own time (during a lunch break for example). No personal use is allowed outside of these times.

Staff using computers linked to the school network or laptops may only use them for personal use in their own time (i.e. before or after directed time or during a lunch break). Please refer to the separate section covering personal use of the Internet.

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. Users will be charged for personal printing in line with a scale of charges. (See the Intranet for details)

Personal use - What Users CANNOT do

- Access Chat Rooms
- Access streaming media (including radio and television)
- Buy music, video etc if it requires a download
- Change settings on School or Council computers
- Create or update a personal website
- Download and / or upload software, images or files
- Download or play games
- Download or play music or videos
- Have goods or services bought online delivered to the workplace
- Use Instant Messaging or Web Messaging
- Use a Council e-mail address to subscribe to websites accessed for personal use
- Use it for private business purposes
- Use it for gambling

The Council 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.

For users of the admin system, the Council's Internet filtering system will allow access to a range of website categories for personal use between the hours of 12:00 – 2:00. These categories will then be blocked outside of the allowed hours (e.g. Shopping, Sports, Travel etc.) Users carrying out transactions online should ensure that they are completed by 2:00pm, as the website will not be available after this time.

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 or Council and must be in accordance with the School or Council's Code of Conduct. This applies for both Council business use and personal use of the Internet.

Social Networking Sites

Staff should not access social networking sites from a School or Council issued computer. Where staff use social networking sites on their own ICT equipment in their private lives, they are requested not to make any reference to school issues or release any sensitive,

confidential or personally identifiable information about staff, pupils or parents. Staff should also be aware of the dangers posed by using such sites and the potential implications on their career. Staff should take suitable action to protect the release of information which could be potentially damaging to themselves or the school. It is also recommended that staff have their privacy settings set as high as they can and do not have past or present pupils and / or parents as friends.

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.

All e-mail and attachments sent and received on School or Council equipment (including personal e-mail) are owned by the Council. 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 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
- All e-mails are potentially subject to disclosure under the Freedom of Information Act
- 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.

What NOT to do when using e-mail

When using the Council's e-mail systems (gateshead.gov.uk and gateshead.org) 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 Council via e-mail

- Enter into a commitment on behalf of the Council unless explicitly 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 Council's Code of Conduct
- have a negative impact on the Council
- interfere with the performance of the user's duties
- result in the Council 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 Council 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 (gateshead.gov.uk and gateshead.org) 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

Management of e-mail records in accordance with the Records Management Policy will help to avoid this situation occurring.

Attachments

- To reduce risks associated with e-mail attachments certain file types are prevented from being sent and received on the Council's e-mail system (gateshead.gov.uk), for example .exe, .bat, .com, .mp3, .scr etc.
- E-mail with attachments larger than 10Mb will be blocked. Users should note that external organisations may also have attachment size limits on their e-mail systems, which may be as low as 2Mb.

Encryption and Digital Signatures

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 make every effort to ensure the privacy of user data, including e-mail messages. Any information obtained by ICT Services 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 will bring this information to the attention of the Council or other relevant authorities.

Telecommunications

Users must contact ICT Services before procuring any items of telecommunications

equipment or software. ICT Services will ensure that all items meet Council standards, are configured securely and are compatible with existing systems.

Telephone systems

All outgoing calls from Council 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 Council 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.

In the Civic Centre and where the facility exists at other Council offices all personal calls must be made using the 174 access code and not the 9 access code.

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

The handset and all equipment remain the property of the Council.

A register of use will be kept for those issued with a school pool mobile phone. Users should sign the phone 'out and in' on the same working day.
All pooled mobile phones should be returned to the school office relevant at the end of each working day or shift or as soon as possible afterwards. Phones should be stored in a locked, secure place in the school office when not issued.

Users are personally responsible for the security and day to day maintenance of the phone.

Losses of handsets or equipment must be reported to the Service Administrative Section immediately. Losses resulting from carelessness may lead to disciplinary action.

The phone must not be used by unauthorised persons.

Private use of the handset is allowed but should be limited to essential calls which must be paid for. Private use will be monitored and any misuse will result in it being withdrawn.

All access to the Internet, television, video, radio and other media, whether for Council business purposes or personal use, must be via a method approved in advance by ICT Services.

Reprographic Equipment

Cameras

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

Printers, Photocopiers & Scanners

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 or scanner.

CCTV equipment

All CCTV equipment must be used in accordance with the relevant legislation.

Disposal of Media and Equipment

All PCs which have become obsolete or are surplus to requirements must have their hard disks checked for content. Software that is being transferred to another machine must be uninstalled and all data files must be deleted.

All data storage files must be purged of sensitive data before disposal or securely destroyed.

All removable media must be rendered unusable before disposal. It should be noted that reformatting does not delete all data from disks and such data can subsequently be removed using freeware.

Hard disks, USB memory sticks and CDs / DVDs containing confidential and / or personal information must be disposed of by a company or agency which meets Waste Electrical and Electronic Equipment (WEEE) Regulation standards.

All paper records can be disposed of through the Council's general waste disposal procedure. However, paper documents containing confidential and / or personal information must first be shredded.

Incident Reporting and Monitoring

Incident Reporting

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

Monitoring of Activity

The School and 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 or Council ICT systems users accept that all use may be monitored.

Review

Policy Reviewed: September 2022
Next Review: September 2024

Appendix 1

Greenside Primary School

Portable Device User's Agreement

I agree to take responsibility for the Portable Computing Device and associated peripherals detailed below. I have read Greenside Primary School's Information Security Policy and agree to comply with its requirements.

The agreement will start when I sign this document below 'date of issue' and will terminate when I return the device and all associated peripherals and sign the Agreement below 'date of return'.

User Information	
Name:	Job Title:
Equipment Information	
Make and Model:	Tag Number:
Peripherals: (List any peripherals issued with the device)	
Sign-off Information	
Date of issue:	Date of return:
User signature:	User signature:
Authorising signature:	Authorising signature:

Appendix 2

Greenside Primary School

Information Security Policy Sign Off

I have read and understand Gateshead Councils ICT Security Policy and agree to abide by it. I am also familiar with, and will adhere to, the Standards, Procedures and Protocols governing the use of the Council's ICT. I understand that violation of any part of the policy may result in disciplinary action being taken against me.

Name	Position in School	Date