Waterloo Primary Academy

ICT Policy Handbook

Approved & Adopted: 24 April 2013
Responsible Personnel: ICT Manager
Policy Last Reviewed/Approved: June 2024
Review Period: Annual
Review Date: June 2025

Zest Academy Trust

Introduction

At Waterloo Primary Academy we are committed to providing the best ICT facilities and services that we can offer both to our staff and students. It is also our aim to continue to enhance the delivery of ICT to aid the learner to become a natural navigator, critical thinker and evaluator, leading to effective communication for all.

The policy is intended to guide and inform staff of how to make best use of the resources available to them. In addition, the policy will aim to give background information regarding security issues and network services.

Legislation

The use of ICT services is governed by several pieces of legislation and it is important that staff are fully aware and understand this.

UK GDPR

In May 2018 the new GDPR came in to force, it replaced the Data Protection Act, however this was superseded by the UK GDPR as of the 1st January 2021, due to Brexit, but the same rules apply.

The act has eight key principles that ensure personal data is:

- **Fairly and lawfully processed**
  To lawfully process information at least one of the conditions in Schedule 2 of the act must be met an in the case of sensitive data being processed one of the conditions in Schedule 3 must also be met.
- **Processed for limited purposes**
  Information held or obtained will only be used for the purpose of the business, and should not be passed on to third party companies, for example, names and addresses should remain secure.
- **Adequate, relevant and not excessive**
  The data that is held on an Individual should not be excessive and should always be relevant to the purpose.
- **Accurate and up to date**
  All personal data should be kept up to date and accurate.
- **Not kept for longer than is necessary**
  Personal data should not be held longer than necessary, for example unsuccessful job application forms.

- **Processed in line with the individuals' rights**
  This principle also covers the right for an Individual to access data that is recorded about them.

- **Secure**
  All individuals' data must be stored securely to safeguard against any unauthorised access.

- **Not transferred to other countries without adequate protection**
  Individuals data should not be transferred to other countries, not all countries are governed by the Data Protection Act.

Companies must comply with The Data Protection Act or could risk being prosecuted.

As the original 1984 Data Protection Act didn't cover the privacy issues, the new legislation that came in March 2000, clearly centres on the Individual Privacy. Employers and large organisations must safeguard the data of others. In addition to the Data Protection Act there are various other Acts and Directives that govern privacy laws, such as;

- The Privacy and Electronic Communications Directive 2003
- The Human Rights Act 1988
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000

Copyright Designs and Patents Act 1988

The Copyright Designs and Patents Act 1998 was introduced to protect a creator's right in which other people may wish to use their work. The Act prevents a person's work from being plagiarised or stolen. It replaces the original Copyright Act that was passed in 1911 and then subsequently amended in 1956; however, some of the original legislation is still currently used within the Act.

The Act is split into seven parts:

- Copyright
- Rights in Performances
- Design Right
- Registered Designs (Amendments of the Registered Designs Act 1949)
- Patents Act and Trademark Agents
- Patents
- Miscellaneous and General

This Act covers software licensing. Individuals can be held legally liable, jointly with the Academy if unlicensed software is used.

Computer Misuse Act 1990

The Computer Misuse Act determines three criminal offences

- **Unauthorised access to computer material**
- **Unauthorised access with intent to commit facilitate commission of further offences**
- **Unauthorised modification of computer material**

Staff must be aware that it is a criminal offence to gain access using an account and password that has not been authorised through the normal procedures – even if the "owner" has supplied the password and account information.

Regulation of Investigatory Powers Act 2000

This act gives employers the right to monitor employee communications in a number of instances, such as;

- interests of national security
- to prevent or detect a crime
- to investigate or detect unauthorised use of telecommunication systems or to obtain evidence of the communications themselves

General Data Protection Regulation

The GDPR came into force on the 25th May 2018, however this was superseded by the UK GDPR as of the 1st January 2021, due to Brexit, but the same rules apply. This is any information that can directly or indirectly identify a natural person, and can be in any format. The Regulation places much stronger controls on the processing of special categories of personal data. The inclusion of genetic and biometric data is new.

- **Personal data**
  The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- **Sensitive personal data**
  GDPR refers to sensitive personal data as "special categories of personal data" The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
- **Data protection by design and by default**
  There is a requirement to build effective data protection practices and safeguards from the very beginning of all processing.
  Data protection must be considered at the design stage of any new process, system or technology.

A DPIA is an integral part of privacy by design.
The default collection mode must be to gather only the personal data that is necessary for a specific purpose.

- **Lawful processing**
  You must identify and document the lawful basis for any processing of personal data. The lawful bases are:
  Direct consent from the individual;
  The necessity to perform a contract;
  Protecting the vital interests of the individual;
  The legal obligations of the organisation;
  Necessity for the public interest; and
  The legitimate interests of the organisation.

- **Valid content**
  There are stricter rules for obtaining consent:
  Consent must be freely given, specific, informed and unambiguous.
  A request for consent must be intelligible and in clear, plain language.
  Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
  Consent can be withdrawn at any time.
  Consent for online services from a child under 13 is only valid with parental authorisation.
  Organisations must be able to evidence consent.

- **Privacy rights of individuals**
  Individuals' rights are enhanced and extended in a number of important areas:
  The right of access to personal data through subject access requests.
  The right to correct inaccurate personal data.
  The right in certain cases to have personal data erased.
  The right to object.
  The right to move personal data from one service provider to another (data portability).

- **Transparency and privacy notices**
  Organisations must be clear and transparent about how personal data is going to be processed, by whom and why.
  Privacy notices must be provided in a concise, transparent and easily accessible form, using clear and plain language.
  Data transfers outside the EU.
  The transfer of personal data outside the EU is only allowed.
  Where the EU has designated a country as providing an adequate level of data protection;
  Through model contracts or binding corporate rules; or
  By complying with an approved certification mechanism, e.g. EU-US Privacy Shield.

- **Data transfers outside the EU**
  The transfer of personal data outside the EU is only allowed;
  Where the EU has designated a country as providing an adequate level of data protection;
  Through model contracts or binding corporate rules; or
  By complying with an approved certification mechanism, e.g. EU-US Privacy Shield.

- **Data security and breach reporting**
  Personal data needs to be secured against unauthorised processing and against accidental loss, destruction or damage.
  Data breaches must be reported to the data protection authority within 72 hours of discovery.
  Individuals impacted should be told where there exists a high risk to their rights and freedoms, e.g. identify theft, personal safety.

- **Data protection officer (DPO)**
  The appointment of a DPO is mandatory for:
  Public authorities;
  Organisations involved in high-risk processing; and
  Organisation processing special categories of data.
  A DPO has set tasks:
  Inform and advise the organisation of its obligations.
  Monitor compliance, including awareness raising, staff training and audits.
  Cooperate with data protection authorities and act as a contact point.

Academy Network

The Academy's network is segregated into the multiple virtual networks. Access to the Academy network is granted through usernames and passwords. It is essential that network security and integrity is maintained and connected devices are not left unattended whilst any user is authenticated.

User Accounts and Passwords

Each member of staff is issued with details of their access permissions to various internal and external systems.

Staff Accounts

The naming convention that is used for accounts is in the following format;

Joe.bloggs	firstname.surname

Pupil Accounts

The naming convention that is used for accounts is in the following format;

Joe.bloggs firstname.surname

Network Access

The access granted to an individual is tailored according to their role and responsibility; therefore, staff and pupils should not divulge details of their account or allow anyone else to use their account. Anyone found to breach this policy will be dealt with through disciplinary procedures.

If a breach is witnessed this should be reported to the IT Manager at the earliest opportunity.

Network Software

The Academy's network infrastructure is at the heart of the business and therefore needs to be secure. Several provisions are in place;

- The Academy building is fully alarmed
- All hardware in Academy is marked with Asset Tags for identification purposes and then added to the Academy's asset register.
- The Servers are located and locked away in the communications rooms and locked data cabinets.
- All Academy software is located in the IT Storage area.
- Mobile devices should either be taken off site or locked away at the end of each day and are the sole responsibility of the teacher.
- Backups are done overnight. Critical business data is backed up offsite. Other data is backed up locally on NAS devices
- Passwords are kept private by the individual and at no time should be shared.
- All Mobile devices should be locked in their designated locations unless a teacher has borrowed them and are therefore become responsible for that piece of equipment.
- The network filtering system monitors and filters unsuitable sites
- There are multiple managed wireless networks which are secured with passwords, certificates and tokens
- Group polices are in place and ensure users can only access the network resources they need.

Email Accounts

All staff are provided with an email account. This includes full email and calendar services. This email account should be the only one that is accessed via the Academy's network; however, the Academy realises that at times other accounts maybe briefly accessed.

Accessing other email accounts from a desktop computer may result in a security exposure for the Academy network as personal accounts are often vulnerable to attacks and or viruses. Some viruses can replicate themselves and spread through email and networks and often masquerade as mail from recognised contacts.

Any files that are attached to an email from an unknown, suspicious of untrustworthy source should not be opened and the ICT Manager should be informed. In addition, any form of SPAM emails should be forwarded to the ICT Manager so that they may then be blocked from the Academy's network.

The Academy has invested in an email gateway and filtering solution, this should stop malicious emails before they reach the inbox of the staff, or student.

Acceptable Use

Staff and students are welcome to use the Academy's network services in accordance with the Academy's Acceptable Use Policy.

Staff should also be aware that there are significant differences between facilities that are available to staff and to students. Should a member of staff or student require access to a site or piece of material that is otherwise filtered, then a request must be forwarded to the School ICT Manager. Staff of students found in breach of the Acceptable Use policy will have their account suspended whilst further enquiries are conducted.

Internet Use

Academy provides filtered access to all staff and students through their personal accounts. The filter used within the Academy network is provided by a core next generation firewall and is managed in house by the ICT Manager. Changes to the filter can be made should a member of staff wish to view a 'banned' page; this can be done via the Risk Management link on the Staff Portal. This process is done to ensure there is an audit trail for changes in the filter. The ICT Manager will review the blocked site to ensure it is suitable for academy use.

The display, distribution, storage, editing and recording of inappropriate material, images or documents or any offensive material is prohibited. It is possible that when using the internet responsibly, staff may find themselves innocently redirected to a different location. If a member of staff finds themselves connected to an inappropriate site they must disconnect from the site immediately and then report the incident to the ICT Manager following guidelines set out in the e-Safety Policy, so that action may immediately be taken place. Chat room access is not granted for either staff of students.

All devices accessing the internet or network services are subject to monitoring including location monitoring. The ICT Manager will, at random select accounts for monitoring and any breaches of policies or inappropriate use will be reported to the Senior Management Team. Inappropriate use of the internet or downloading of files for personal use which impacts an individual's professional responsibilities and / or impacts on the academy will be considered a misuse of the facility. Therefore, all staff and students must comply with the Academy's Internet Use Policy and Acceptable Use Policy.

Computer Maintenance

Any problems with ICT equipment or services should be via the Risk Management link. This is done so that an audit trail of maintenance may be kept.

No food or drink is to be consumed or placed around any ICT equipment.

Backup Procedures

Backups at Waterloo Primary Academy are completed daily.

Business Critical Data

Data is backed up off site daily. This includes data contained within Sims.NET.

Servers

There are multiple servers in the Academy that store user data including system generated content. This is backed up daily to NAS devices for maximum redundancy, other systems are backed up to a cloud backup system.

Email Server

Email is provided by Office 365. Although this is a highly available system and data. Loss is extremely unlikely, backups are not provided by the services and it is recommended that uses backup their email on a regular basis.

Printing

The facility to monitor and restrict printing within Academy is currently in place, which limits staff and students alike.

Laptop Loan Scheme

Academy provides devices for those members of staff who require one. Staff are advised that as part of the loan scheme stipulations, they are required to connect to the Academy's network at least once a week so that their anti-virus and software may be updated.

Staff are also aware that they are responsible for the security of the loan device and are personally responsible for insurance when taking off-site. Staff must agree that damages resulting in a devices misuse or as a result of failing to secure a device, may result in repair or replacement costs being deducted from salaries.

Health and Safety

When using computer equipment for an extended period of time it is advisable to consider some health and safety aspects;

- Take regular breaks from working at your computer – a few minutes at least once an hour, stand up stretch, move around
- Alternate work tasks
- Regularly stretch to relax your body
- Keep your mouse and keyboard at the same level
- Check your seating position, do not slouch, make sure your lower back is supported
- Avoid bending or angling your wrists while typing or using a mouse
- All users should complete a DSE Workstation checklist
- Any issues arising from the DSE check should be raised with the ICT Manager

All these points of advice are taken from the computer health and safety website.

Acceptable Use Policy

All devices / systems are owned by the Academy and are made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The Academy's Internet Access Policy has been drawn up to protect all parties - the students, the staff, and the Academy.

The Academy reserves the right to examine or delete any files that may be held on its computer system or to monitor any use including the ability to remotely trace, lock or wipe devices.

Anyone using the academy's network services is bound by the Acceptable Internet Use policy.

- All Internet activity should be appropriate to staff professional activity or the student's education.
- Access should only be made through the authorised username, password, which should not be made available to any other person;
- Activity that threatens the integrity of the Academy systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- As an e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Under no circumstances should students or staff open or tamper with any item of Academy equipment including removal of safety or protective equipment.
- Users should not connect or alter any device connections

- Under no circumstances should students or staff attempt to install any software or apps on the Academy network
- User areas are randomly scanned for filenames which are abusive and data which is not for student or staff use.
- Under no circumstance are users allowed to download any software or obscene material using the internet.