# Zest Academy Trust

## Information Security Policy

*Incorporating the Data Breach Plan & Information Classification & Handling Procedure*

Approved & Adopted By Trust Board: 19/06/2018
Review Period: Biennial
Policy Date Last Reviewed/Approved 20/02/2023
Person Responsible: COO
Version Number: 1

# Information Security Policy

## Contents





Version 1 Last Updated 20/02/2023
Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 Registered in England No. 8087508

## Introduction

Waterloo Primary Academy is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

When processing personal information, under the UK General Data Protection Regulation (UK GDPR), the School/Academy/Trust must:

- use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage
- implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Academy's data processing activities; and
- be able to demonstrate that it has used or implemented such measures.

The purpose of this policy is to:

- protect against potential breaches of confidentiality
- ensure the integrity and availability of all our information assets and IT facilities by protecting them against damage, loss or misuse
- support the Academy's Data *Protection Policy* by ensuring all staff are aware of and comply with UK law and the Academy's procedures relating to the processing of personal information; and
- increase awareness and understanding of the requirements of information security and the responsibility of staff to protect the confidentiality, integrity and availability of the information that they handle.

## Definitions

For the purposes of this Policy, the following definitions apply:

**'business information'** means business-related information other than personal information relating to staff, parents, pupils, service providers and suppliers and other business contacts of the Academy.

**'confidential information'** means any information other than personal information that is key to the operation of the Academy. The loss or disclosure of which could cause harm to the organisation.

**'personal information'** (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information.

**'pseudonymised'** means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.

**'sensitive personal information'** (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

## Roles and Responsibilities

Information security is the responsibility of all staff. The Academy's data protection manager together with the data protection officer is responsible for:

- monitoring and implementing this policy;
- monitoring potential and actual security breaches;
- ensuring that staff are aware of their responsibilities; and
- ensuring compliance with the requirements of the UK GDPR and other relevant legislation and guidance.

## Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Academy, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

This policy applies to all staff, including governors & trustees, staff, temporary and agency workers, contractors, interns, volunteers and apprentices.

All staff must be familiar with this policy and comply with its terms.

The information covered by this policy may include:

- personal information relating to staff, parents, pupils and other stakeholders
- other business information; and
- confidential information.

This policy supplements the Academy's Data Protection Policy and other policies and privacy notices and all other policies and procedures relating to the handling and processing of information, the use of ICT and retention schedules. The contents of those policies and procedures must be taken into account, together with this policy.

We will review and update this policy on an annual basis or as necessary in response to changes in the regulatory environment and/or our handling and processing activities. This policy does not form part of any staff member's contract of employment, and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

## General Principles

All Academy information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

Personal information, and sensitive personal information, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

Academy information (other than personal information) is owned by the Academy and not by any individual or team.

Academy information must be used only in connection with work being carried out for the Academy and not for other commercial or personal purposes.

Personal information must be used only for the specified, explicit and legitimate purposes for which it is collected.

## Information Management

Personal information must be processed following:

- the data protection principles, set out in the Data Protection Policy

- the Data Protection Policy, generally; and
- all other relevant policies and procedures.

In addition, all information collected, used and stored must be:

- adequate, relevant and limited to what is necessary for the relevant purposes
- kept accurate and up to date.

The Academy will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

- pseudonymisation of personal information (where appropriate)
- encryption of personal information

Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed following the Academy's data retention schedule.

## Human Resource Information

Given the internal confidentiality of personnel files, access to such information is limited to the HR Department Except as provided in individual roles, other staff are not authorised to access that information.

Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

Staff may ask to see their personnel files and any other personal information under the UK GDPR and other relevant legislation. For further information, see the Academy's *Individual Rights Policy and Procedure*.

## Access to Offices Information

Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party.

Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, eg through office windows.

Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.

Wherever possible, visitors should be seen in meeting rooms. If a member of staff must meet with visitors in an office or other room which contains Academy information, then steps should be taken to ensure that no confidential information is visible.

At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

## Computers and IT

Password protection and encryption must be used where available on Academy systems to maintain confidentiality.

Computers and other electronic devices must be password protected and those passwords must be changed regularly. Passwords must not be written down or given to others.

Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

Confidential information must not be copied onto a removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of the Head of School and must be encrypted. Relevant data held on such devices should be transferred to the Academy's computer network as soon as possible for it to be backed up. It should then be deleted from the device.

All electronic data must be securely backed up at the end of each working day.

Staff must ensure they do not introduce viruses or malicious code into Academy systems. Software must not be installed or downloaded from the internet without it first being virus checked and authorised by the ICT Manager

Staff should contact The IT Manager for guidance on appropriate steps to be taken to ensure compliance.

## Communications and Transfer of Information

Staff must take care to maintain confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.

Confidential information must be marked 'confidential' and circulated only to those who have a 'need to know' during the course of their work. (See the *Information Classification and Data Handling Procedure* in appendix 3, below).

Confidential information must not be removed from the Academy offices unless required for authorised business purposes.

Where confidential information is permitted to be removed from the Academy offices, all reasonable steps must be taken to ensure that the integrity and confidentiality of the information are maintained. Staff must ensure that confidential information is:

- stored on an encrypted device with strong password protection, which is kept locked when not in use
- when in paper copy, not transported in see-through or other unsecured bags or cases
- not read in public places (e.g. waiting rooms, cafes, trains); and
- must remain in contact with the staff member at all times while in transit (e.g. not left unattended in luggage racks or in any place where it is at risk such as conference rooms, car boots, cafes, etc.).

Postal, document exchange (DX) and email addresses should be checked and verified before the information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

All sensitive or particularly confidential information sent by email should be encrypted or attached as a password-protected document.

All sensitive or particularly confidential information sent as hard copy must be posted by recorded delivery

## Personal Email and Cloud Storage Accounts

Personal email accounts, such as Yahoo, Google or Hotmail and cloud storage services, such as iCloud and OneDrive are vulnerable to hacking. They do not provide the same level of security as the services provided by the Academy's own IT systems. Do not use a personal email account or cloud storage account for work purposes.

If you need to transfer a large amount of data, contact IT for assistance

## Home Working

Staff must not take Academy information home unless required for authorised business purposes,

Where staff are permitted to take Academy information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

- personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all personal and confidential information must be retained and disposed of in following the Trust's Records Management and Retention Schedule and Policy.

Staff must not store confidential information on their home computers (PCs, laptops or tablets).

Refer to the Academy's Working at *Home* Policy for further information.

## Transfer to Third Parties

Third parties should be used to process Academy information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether a third party will be processors. A controller or a joint controller under the UK GDPR.

Staff involved in setting up new arrangements with third parties or renewing/altering existing arrangements should consult the DPO for more information.

## Overseas Transfer

The Data Protection legislation restricts international transfers of personal information and transfers to international organisations. Staff may only transfer personal information outside the UK, or to an international organisation, with the prior written authorisation of the senior leadership team.

You should refer to the Academy's *Data Protection Policy* for further information on international transfers. Staff involved in setting up data transfer arrangements should consult the DPO for more information.

## Reporting Breaches

All members of staff must report actual, suspected or potential data protection compliance failures. This allows the Academy to:

- investigate the failure and take remedial steps if necessary
- maintain a register of compliance failures; and
- make any applicable notifications.

Please refer to the breach procedure (Appendix 1, below) for further guidance

## Consequences of Failure to Comply with this Policy

The Academy takes compliance with this policy very seriously. Failure to comply with it puts both staff and the Academy at significant risk. The importance of this policy means that failure to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

Staff with any questions or concerns about anything in this policy should not hesitate to contact the DPO or Nicola Lea HR Business Manager.

# Appendix 1: Data Breach Plan

## Introduction

This personal data breach plan:

- places obligations on staff and others who work for or on behalf of Waterloo Primary Academy to report all actual or suspected personal data breaches; and
- sets out our procedure for managing and recording actual or suspected breaches.

This plan applies to all staff, and to all personal data and special category personal data held by the Academy.

This plan supplements our policies relating to Data Protection and Information Security.

## Key Terminology

**'Personal data breach'** means a breach of data security leading to the accidental loss, destruction, theft, corruption, or unauthorised disclosure of personal data transmitted, stored or otherwise processed by the Academy.

**'Personal data'** means information relating to a living individual who can be identified (directly or indirectly) from that information.

**'Data subject'** means the individual to whom the personal data relates.

**'Special category data' (sometimes known as sensitive personal data)** means personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, biometric data and data concerning health, sex life or sexual orientation

'**Data protection officer** (DPO)' or '**Data protection manager** (DPM)' means the person appointed to lead OR be involved in:

- the development and implementation of our data protection; and

- data privacy strategy and compliance with the UK GDPR and other applicable laws.

**'Data breach team'** means the team responsible for managing and investigating personal data breaches**.**

**'Information Commissioner's Office (ICO)'** means the UK's independent data protection regulator.

## Responsibility

The internal data protection manager together with the external data protection officer has overall responsibility for this plan. They are responsible for ensuring it is complied with by all staff.

## Our Duties

The Academy processes personal data relating to individuals including staff, pupils, parents and other stakeholders. As custodians of data, we have a responsibility under UK data protection law to protect the security of the personal data we hold.

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies in particular our *Data Protection Policy and Information Security Policy*.

## What Can Cause a Personal Data Breach?

A personal data breach can happen for several reasons:

- loss or theft of data or equipment on which data is stored, e.g. loss of a laptop or a paper file
- inappropriate access controls allowing unauthorised access and use
- loss of availability of personal data owing to equipment failure
- human error, e.g. sending an email to the wrong recipient
- unforeseen circumstances such as a fire or flood

- hacking, phishing and other ‘blagging’ attacks where information is obtained by deceiving whoever holds it; and,
- accidental or deliberate alteration of personal data

## If you are Responsible for a Personal Data Breach?

If you inadvertently caused a personal data breach, consider if there are immediate steps you can take to contain the breach. For example, if you have sent an email to the wrong person internally, recall the email. If the email has been sent externally, try contacting the recipient by telephone and ask them to delete the email without opening it, and to confirm the deletion to you in writing.

## Managing Recording the Breach

On being notified of a suspected personal data breach, the DPO will work with the data breach team (see Appendix 2**),** to establish whether a personal data breach has occurred. If so, the data breach team will take appropriate action to:

- contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed
- assess the risk and record the breach in the Academy’s data breach register
- notify appropriate parties of the breach in certain circumstances; and,
- take steps to mitigate future breaches.

These are actions are explained more fully below.

## Containment and Recovery

The data breach team will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of personal data.

The data breach team will identify ways to recover, correct or delete data. This may include contacting the police where the breach is related to stolen hardware or data.

Depending on the nature of the breach, the data breach team will notify the Academy's professional indemnity insurer, cyber insurer and/or crime insurer as the insurer can provide access to data breach management experts.

## Assess and Record the Breach

Having dealt with containment and recovery (see above), the data breach team will assess the risks associated with the breach, including:

- the categories of data and quantity of data involved
- the sensitivity of the data
- the categories and number of data subjects involved
- where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?
- could it be used for harmful purposes?
- what could the data tell a third party about the data subject?
- the likely consequences of the breach on affected data subject/s
- the likely consequences of the breach on the Academy

Details of the breach will be recorded in the Academy's data breach register by the data breach team.

## Notifying Appropriate Parties about the Breach

Based on the assessment of the breach the data breach team will consider whether to notify:

- the ICO
- affected data subjects
- the police
- the LA, DfE or other relevant stakeholders

- any other parties, e.g. insurers.

## Notifying the ICO

The data breach team must inform the ICO when a personal data breach has occurred if the assessment of the breach indicates it is likely to result in a high risk to the rights and freedoms of data subjects. Such detriments include discrimination, reputational damage, emotional distress, and physical or financial damage. For example:

- a risk to physical safety:
- exposure to identity theft through the release of non-public identifiers, e.g. passport numbers, driving licence numbers, etc.
- information about the private aspects of a person's life becoming known to others, e.g. financial circumstances.

The volume of personal data is also a consideration when assessing whether to notify the ICO, there should be a presumption to report to the ICO where:

- a large number of data subjects are concerned, and/or
- multiple categories of personal data,
- there is a real risk of individuals suffering some harm.

It may, however, be appropriate to report lower volumes in circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves **special category personal data.** If the information is particularly sensitive, even a single record could trigger a report. For example, the theft or loss of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable.

Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

If the data breach team is unsure whether to report, the ICO provides a helpful breach assessment tool. In cases where uncertainty remains the presumption should be to report.

## Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach team will notify the affected data subject(s) without undue delay, including:

- the categories of data breached
- the name and contact details of the data protection officer or another contact point where more information can be obtained
- the likely consequences of the personal data breach; and
- the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

When determining whether and how to notify data subjects of the breach, the data breach team will:

- co-operate closely with the ICO and other relevant authorities, e.g. the police where necessary
- take account of the factors set out in the table below:

| Factor | Subject |
|---|---|
| Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption. | Where such measures have been implemented, it is not necessary to notify the data subject(s). |
| Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.<br><br>Whether it would involve a disproportionate effort to notify the data subject(s).<br><br>Whether there are any legal or contractual requirements to notify the data subject?<br><br>Whether it would involve a disproportionate effort to notify the data subject(s).<br><br>Whether there are any legal or contractual requirements to notify the data subject? | Where such measures have been implemented, it is not necessary to notify the data subject(s).<br><br>If so, it is not necessary to notify the data subject(s) individually—but we must instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.<br><br>If yes, it may be necessary to notify the data subject(s) in any event.<br><br>If so, it is not necessary to notify the data subject(s) individually—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner<br><br>If yes, it may be necessary to notify the data subject(s) in any event. |

## Notifying the Police

The data breach team will already have considered whether to contact the police for the purpose of containment and recovery (see above). Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the data breach team will notify the police and/or relevant law enforcement authorities.

## Notifying Other Parties

The data breach team will consider whether there are any legal or contractual requirements to notify any other parties, e.g. the governing body, Local Authority, Department for Education, etc.

## Preventing Future Breaches

Once the personal data breach has been dealt with, following this plan, the data breach team will:

- establish what security measures were in place when the breach occurred
- assess whether technical or organisational measures can be implemented to mitigate similar breaches from happening again
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- consider whether it is necessary to conduct or update the relevant privacy impact assessment
- update the privacy risk register; and
- debrief the data breach team members.

## Monitoring and Review

We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate every year

Monitoring and review exercises will include looking at how policies and procedures are working in practice to reduce the risks posed to our Academy.

## Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding.

We provide regular training to staff:

- at induction;
- when there is any change to the law, regulation or internal policy or processing activity
- when significant new threats are identified; and
- in the event of an incident affecting our Trust or the sector.

## Reporting Concerns

Prevention is always better than cure.

Data security concerns may arise at any time, and we encourage staff to report any concerns to the *data protection Manager or the Data Protection Officer*. This helps us capture risks as they emerge, improve our information security practices, protect our stakeholders from personal data breaches and keep our processes up-to-date and effective.

## Consequences of Non-Compliance

Failure to comply with this plan and associated policies (e.g. the Data Protection or Information Security policies) put you and Academy at risk. Failure to notify the [DPM or DPO] of an actual or suspected personal data breach is a very serious issue.

You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.

## Data Breach Team

| | |
|---|---|
| Data Breach Team Lead | External DPO: The Schools People |
| Data Protection Manager | N Lea |
| ICT & Network Manager | L Warren |
| Site Manager/Physical Security | P Johnson |

## Appendix 2: Data Security Incident/Breach Form

**Reference Number: XXX/XXX/XXX**

# Data Security Incident/Breach Form

**To be completed in all instances of an actual or suspected Data Security incident/breach**

Please act promptly to report any actual or suspected data security incident or data breach by notifying your line manager immediately. Complete sections 1 & 2 and email this form to the Data Protection Manager Nicola.Lea@zestacademytrust.co.uk

| **Section 1: Notification of Data Security Incident/Breach**<br>*To be completed by the line manager of the person reporting the incident* | |
|---|---|
| Date incident was discovered: | |
| Date(s) of incident: | |
| Place of incident: | |
| Name of person reporting the incident: | |
| Contact details of the person reporting the incident (email address, telephone number) | |
| Brief description of the incident or details of information lost: | |
| The number of Data Subjects affected: | |

| | |
|---|---|
| Has any personal data been placed at risk? If so, please provide details | |
| Has any Special Category Data been placed at risk? If so, please provide the details: | |
| Brief description of any containment action taken at the time of discovery e.g. email recall, computer shutdown etc. | |
| ***For use by the Data Protection Officer*** | |
| | |

| | | | |
|---|---|---|---|
| Received by: | | Date: | |
| Forwarded by | | Email:<br>Telephone: | |
| Lead Investigating Officer appointed | | Email:<br>Telephone: | |
| **Section 2: Assessment of Severity**<br>*To be completed by the Lead Investigation Officer in consultation with the Head of the area affected by the breach and if appropriate IT where applicable* | | | |
| Details of the IT systems, equipment, devices, records involved in the security breach: | | | |
| Details of hard copy data involved in the security breach | | | |
| ***Details of Information loss (defined as unrecoverable e.g, not backed up)*** | | | |
| How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems? | | | |

| | |
|---|---|
| Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Company or third parties? | |
| How many data subjects are affected? | |
| Is the data bound by any contractual security arrangements? | |
| ***What is the nature of the data involved?*** *Please provide details of any types of information that fall into any of the following categories:* | |
| HIGH-RISK personal data<br>Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's<br>a) racial or ethnic origin;<br>b) political opinions or religious beliefs;<br>c) trade union membership;<br>e) biometrics (where used for ID purposes)<br>f) health;<br>g) sex life or sexual orientation | |
| Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; | |
| Personal information relating to children and vulnerable adults; | |
| Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed | |
| Information about individual cases of investigations, discipline or sensitive negotiations that could adversely affect individuals. | |

| | |
|---|---|
| Security information that would compromise the safety of individuals if disclosed. | |
| Other | |

| **Section 3: Action Taken**<br>***To be completed by Data Protection Officer and/or Lead Investigation Officer*** | | | | |
|---|---|---|---|---|
| Was the incident reported to the police | | | YES/NO | Date Reported |
| Incident number | | Completed by | | |
| Follow-up<br>action required/recommended: | | | | |

| | | | |
|---|---|---|---|
| Notification to ICO | YES/NO | Date reported | |
| Details of notification | | | |

| | | | |
|---|---|---|---|
| | | | |
| Notification to Data Subjects | YES/NO | Date reported | |
| Details of notification | | | |
| Notification to Other Stakeholders | YES/NO | Date reported | |
| Details of notification | | | |

| Evaluation and Response | Date report completed | |
|---|---|---|
| | | |

## Appendix 3: Information Classification and Handling Procedure

### Why is this important?

Waterloo Primary Academy uses large volumes of information to support its activities and to achieve its strategic aims. Information that the Academy manages shall be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal requirements.

To protect information consistently, it is necessary to define an Academy wide scheme for classifying (describing) information and how it should be handled according to its requirements for confidentiality, integrity, and availability.

The School should classify information so that it is clear to everyone with access to know how best to protect it.

Everyone with access to Academy data should use the Information Classification and Handling Procedure.

### What is the information and handling procedure?

The procedure describes how information and systems should be classified and marked, according to their confidentiality, criticality or value. Decisions around the appropriate protection and use of the information in each classification are based on the consequences of the loss or disclosure of the information.

The procedure relates to all types of information and formats and applies in particular to staff and also to third-party processors wherever appropriate.

The Academy recognises that there may be legitimate circumstances where it is not possible to adhere to this procedure. In these cases, you must seek advice from your line manager.

### What do I need to do?

You should assess the sensitivity of the information you create and receive using the table in Annex A, and take proportionate measures to ensure that information is used and accessed securely – the key controls for protecting information are available in Annexes B and C.

Where information classified as Protected, Restricted or Reserved is shared with others for a valid business reason, everyone should ensure that the recipient is aware of the information's classification and their obligation to protect it.

Access to information in the Protected, Restricted or Reserved classifications by a third party requires a data sharing or confidentiality agreement in place, signed on behalf of the Academy and the other party.

## What if something goes wrong?

The Academy is expected to inform the Information Commissioner's Office of any significant information security breach relating to personal data under the UK GDPR and the Data Protection Act (2018) and must report any significant breaches relating to other types of 'sensitive' information to the data owner and other relevant parties.

The Academy recognises that failure to adhere to its legislative, regulatory and contractual obligations may result in significant financial and legal penalties and reputational damage. It is therefore vital that everyone reports any observed or suspected security incidents including where a breach of the School's security policies has occurred and any security weaknesses in, or threats to, systems, processes or services.

Any actual or suspected information security breaches must be immediately reported by informing the Data Protection Manager or the External Data Protection officer.

## Contacts

| | |
|---|---|
| Data Protection Manager: Nicola Lea. | Email Nicola.Lea@zestacademytrust.co.uk |
| Data Protection Officer: Dee Whitmore. | Email: DPOService@schoolspeople.co.uk |
| | Tel: 01773 851 078 |
| Information Commissioners Office: | https://ico.org.uk/ |
| | Tel: 0303 123 1113 |

Zest Academy Trust

## Appendix A: Data Classification

| School Information Classifications | | | | |
|---|---|---|---|---|
| Classification: | Public | Protected | Restricted | Reserved |
| Risk | ***None*** - confidentiality is of no particular significance to this information | **Low** – inappropriate disclosure would have minimum risk | ***Medium*** - inappropriate disclosure could adversely affect the School's reputation or operations, cause substantial distress to individuals or breach statutory restrictions on disclosure of information, resulting in likely financial or legal penalties | ***High*** – inappropriate disclosure could cause significant damage to the School's reputation or operations, cause great distress to individuals, pose a danger to personal safety or to life or impede the investigation or facilitate the commission of a serious crime, and result in substantial financial or legal penalties. |
| Access | May be viewed by anyone, anywhere in the world and includes information required under the Freedom of Information Publication Schedule | Available to all relevant School staff (e.g. secured behind a login screen) | Available only to specified authorised staff members (e.g. secured behind a login screen, requires authorisation to gain access) | Access is controlled and restricted to a small number of authorised staff members (e.g. secured behind a login screen, requires authorisation to gain access) |
| Personal Information examples (not exhaustive) | Anonymised Information[1]<br>Staff Details shared publicly by the School<br>Information on individuals made public with consent including on social media | Pupil Names and Email addresses<br><br>Staff Work Contact Details (incl. job titles)<br><br>List of Pupil or staff names and ID number | Individual's home addresses, contact details, and passport or NI numbers<br><br>Individual's name, home addresses, contact details and age<br><br>Images including CCTV footage<br><br>Pupil registration and attendance details<br>Comments on pupils' performance | Financial information relating to individuals e.g. banking information, and salary details.<br><br>Information on an individual's racial or ethnic origin, political option, religious or other beliefs, physical or mental health or criminal record<br><br>Staff appointment, promotion or details of personal affairs |

| | | | | |
|---|---|---|---|---|
| | | | Prospective pupils' contact details, References[2] | |
| | | | Individual's name plus DoB or national insurance number (NI)[2] | Individual's name plus DoB or NI number, passport details, home address and telephone number3 |
| Non-Personal Information examples | | | Information relating to the supply or procurement of goods/services before approved publication[4] | |
| | Anything subject to disclosure under the Freedom of Information Act Marketing or Press Information. Factual and general organisational data for public dissemination incl. annual reports or accounts | HR Policies and Guidance | Computer passwords | Legal advice or other information relating to legal action against or by the School |

1. For these purposes anonymised information is information which cannot identify an individual either in isolation or when combined with other information.
2. Content dependent e.g. information relating to health, criminal record or disciplinary matters would make the reference or form Reserved
3. Adding additional combinations of data can change the overall classification (sensitivity) of the information. Increasing the volume can also increase the classification level.
4. The classification of a document may change as is moves through the procurement process

## Appendix B: Handling Paper or Other Portable Media

| | School Information Classifications | | | |
|---|---|---|---|---|
| Activity | Public | Protected | Restricted | Reserved |
| Creation | N/A | N/A | Visibly marked 'CONFIDENTIAL' | Visibly marked 'STRICTLY CONFIDENTIAL'<br>To be created (and stored) only in a secure environment.<br>Copies are to be limited, numbered and recorded.<br>Copies delivered by hand. |
| Storage in School | N/A | A locked filing cabinet or equivalent | A locked filing cabinet or equivalent in an office which is locked or attended at all times during working hours | A locked filing cabinet or equivalent in an office which is locked or attended at all times during working hours |
| Can take off or around the site | Yes | For the shortest time possible. Documents are to be kept securely and in contact with the person at all times | For the shortest time possible. Documents are to be kept securely and in contact with the person at all times | Only exceptionally and with authorisation from the line manager.<br>Documents are to be kept securely and in contact with the person at all times |
| Can Post | Yes | Yes | Double envelope with an inner envelope marked as stated above.<br>Hand-delivered, recorded or courier delivery | Double envelope with an inner envelope marked as stated above,<br>Hand-delivered, recorded or courier delivery |
| Disposal | Recycling | Recycling (shredding if available) | Crosscut Shredding, Confidential Waste disposal | Crosscut Shredding, Confidential Waste disposal |

## Appendix C: Handling Electronic Data

| | School Information Classifications | | | |
|---|---|---|---|---|
| Activity | Public | Protected | Restricted | Reserved |
| Creation | N/A | N/A | Visibly marked 'CONFIDENTIAL' | Visibly marked 'STRICTLY CONFIDENTIAL';<br>To be created (and stored) only in a secure environment<br>Copies are to be limited, numbered and recorded |
| Can Email | Yes | Yes | Only as an encrypted/password-protected attachment<br>The password is to be communicated via a different communication medium (text, phone call)<br>Take care to check the recipient(s) email addresses | Only as an encrypted/password-protected attachment<br>The password is to be communicated via a different communication medium (text, phone call)<br>Take care to check the recipient(s) email addresses |
| Need to Password Protect file in transit | N/A | N/A | Transport on a password-protected device<br>Password for the device and file to meet the School standard | Transport on a password-protected device<br>Password for the device and file to meet the School standard |
| Can access remotely | Yes, via an authentication gateway server and folders have permissions applied, which only allows access to authenticated users. | Yes, via an authentication gateway server and folders have permissions applied, which only allows access to authenticated users. | Yes, via an authentication gateway server and folders have permissions applied, which only allows access to authenticated users. | Yes, via an authentication gateway server and folders have permissions applied, which only allows access to authenticated users. |

| | | | | |
|---|---|---|---|---|
| Can keep on School laptops or other portable media | Yes | Only temporarily, taking care to avoid loss or theft | Only temporarily and if encrypted/ password protected, taking care to avoid loss or theft | Only temporarily and if encrypted/password protected, taking care to avoid loss or theft |
| Can keep on personally owned devices if School Policy permits | Yes | No | No | No |
| Store on School servers | Preferably in backed-up personal or shared network spaces | Only in backed-up personal or shared network spaces with access restricted to only those with a valid right to access the information either by adding a password to the document, encrypting it or applying permissions to a folder. | Only in backed-up personal or shared network spaces with access restricted to only those with a valid right to access the information either by adding a password to the document, encrypting it or applying access controls/ permissions to a folder. | Only in backed-up personal or shared network spaces with access restricted to only those with a valid right to access the information either by adding a password to the document, encrypting it or applying access controls permissions to a folder. |