Assessment, Recording and Reporting Policy

‘Together we are stronger’

CONTENTS

1.0 Roles and Responsibilities

The responsibility for the implementation of this policy and provision rests with the Principal. On an operational basis, the management, responsibility and evaluation of this policy will be undertaken by the Vice Principal.

2.0 Suggested Audience

All teaching and support staff, parent/carers and students. As part of their academy induction or professional development, all staff will participate in training which will enable them to use the knowledge, principles and procedures outlined in this policy.

3.0 Related policies

This policy is part of a suite of policies which should also be referred to:

- Academy Development Plan: Key Performance Indicators (KPIs) and targets
- Equal opportunities for students
- Mentoring and guidance of students

4.0 Academy Mission Statement

'Together we are stronger'

5.0 Introduction

5.1 This academy is a member of the Delta Academies Trust (DAT). The academy will use the resources and expertise of the DAT and work closely with other DAT academies to ensure that this policy is implemented using best practice. It is the aim of Rossington All Saints Academy that every student achieves the very highest level of attainment which reflects their ability.

5.2 Assessment is the tool by which this academy will judge the attainment of individuals and groups of students, set targets for each student and measure progress towards each student achieving their potential. This will enable staff to calculate the academy's performance and hence judge the overall effectiveness of the provision.

5.3 Efficient, up-to-date and accessible online recording systems will allow all staff in the academy to work with accurate information about individual students to help them achieve at least at the level of national expectation.

5.4 Accurate recording systems will allow for statistical analyses to be performed regularly providing information for target setting and the predictions of outcomes.

6.0 The Academy Framework

The academy framework for assessment, recording and reporting aims to:

- collect and provide meaningful data that is clearly presented to its audience of students, parents/carers and staff;

- make effective use of student data for manageable communication with students and parents/carers and between staff; and

7.0 Leading the system

7.1 This system is led by the Vice Principal who works closely with other academy leaders to establish a standardised and moderated system understood by all staff. These academy leaders will work with their teams in analysing progress in attainment and attitude, to ensure that prioritised intervention takes place, the impact of which is then monitored.

8.0 Target Setting and Data Handling

8.1 An essential part of improving achievement is to set and agree targets with each student that are aspirational. Targets and progress being made towards them will be discussed regularly with students and their parents/carers.

- Targets set will be aspirational and ensure that students are given the opportunity to maximise their potential.

- Parents/carers receive information about progress of their child against agreed targets through the academy reporting schedule and at parents'/carers' consultation meetings.

- The Education Advisory Board will receive information on students' progress throughout the year, to enable it to make informed decisions when agreeing targets and monitoring and evaluating progress.

8.2 Target grades are set in all subjects for end of year (KS3)/Years 7 and 8 or end of course (Years 9 to 13) (KS4 and post-16). For KS3 they are based on KS2/Year 6 core subject performance. The expectation in targets is for students to make at least 2 Progress Steps per year. For KS4, the targets are based on KS2 results, again with 10 Progress Steps (2 per year) across their time at the academy as a minimum expectation. At post-16 targets are generated through L3VA predictions, which is consistent across the C6 Partnership.

9.0 Assessment for Learning (AfL) and Assessing Pupils' Progress (APP)

9.1 **Assessment for Learning (AfL).** The academy will build on the work from the predecessor school and from DAT's other academies. Assessment for Learning will be a whole-academy strategy, which will reflect the ten core principles of the National Strategy in this area. Eg:

- Focuses on how students' learn
- Is central to classroom practice
- Is part of effective lesson planning
- Helps students know how to improve
- Develops the capacity for peer- and self-assessment
- Fosters motivation

10.0 Reporting to Parents/Carers

10.1 Progress sheets will be sent home in each cycle either directly with students or made available electronically on the parent portal. Overall behaviour in lessons can be seen from the criteria referenced 'Mindset for Learning' levels.

10.2 Students will also be able to access their own data.

10.3 Years 7-11 are invited to at least one Subject Parents' Evening each academic year, with additional evenings offered where appropriate e.g. Y7 students meeting House Directors, additional Y11 Parents' Evenings etc.

10.4 Year 11 have ongoing consultative evenings, led by departments throughout Year 11, as part of a planned programme.

10.5 In addition to the individual student and subject level of data analysis, whole academy analysis of data takes place at each cycle end with monitoring of:

- Projected 5+ E/M
- Progress 8 data
- Attainment 8 data
- Projected progress of students following the EBac route in terms of curriculum provision.
- Projected 3 & 4+ levels progress KS2 – 4, divided by starting level and across core subjects
- Projected 3 & 4+ levels of progress for Maths and English
- Progress of students in key groups of students e.g. Pupil Premium, gender, MAAT
- Analysis of progress relative to KS2 starting point for all KS3 subjects, with regard to average point score (APS).

11.0 Training and Professional Development

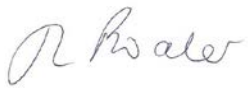
- All staff (including trainee teachers) will receive an induction session on assessment, recording and reporting on joining the academy and the implementation of the policy will be monitored.
- Staff will be encouraged to share and experience effective practice.
- Assessment, recording and reporting training will be available to staff throughout the year.
- The Academy will make use of best practice. E.g. TEEP (Teacher Effectiveness Programme) to improve the understanding and skills of staff in this area
- Staff will be encouraged to accredit any relevant practitioner research, which may be counted as part of a future MA (Teaching and Learning) qualification.
- The SLT will regularly review whether relevant whole staff training is required.

12.0 Monitoring and Review

The designated Vice Principal will monitor the implementation and effectiveness of this policy.

13.0 Approval by the EAB and Review Date

This policy has been formally approved and adopted by the EAB at a formally convened meeting

Policy approved: 

(Chair of Local Governing Body)

Date: 12/12/2016

Date of Policy review: 12/12/2017

Appendix 1: Data-handling Do's and Don'ts

1 Introduction

This summary document includes the key messages in *Data Handling Procedures in Government* and *HMG Security Policy Framework* for those in the education and skills sector. It is intended for leaders, senior leadership teams, network managers and other members of staff who have responsibility for handling and securing data.

The underlying principle of our guidance is that through a combination of technical and procedural solutions, organisations should do everything within their power to ensure the safety and security of any personal data (or data that is important to the secure running of an organisation).

In following this guidance, the reader will be able to identify:

- data and information assets (data, stored in any manner, which is recognised as important or 'valuable' – not just in financial terms – or important to the organisation), with named owners responsible for them
- a framework for ensuring data is correctly marked, managed and secured
- methods for the systematic assessment of risks and recording of data loss so that appropriate mitigating measures can be established.

2 Who is responsible and what data handling changes are required?

Data Handling Procedures in Government highlighted two roles that have responsibility for information security risk management. Organisations may already have staff with different titles who carry out these roles. However, we strongly recommended that organisations adopt the titles below (and the responsibilities attached to them).

2.1 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is a senior member of staff who is familiar with information risks and the organisation's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs)
- They act as an advocate for information risk management.

2.2 Information Asset Owner (IAO)

Organisation should identify their information assets. These will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence. The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations.

Organisations should then identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate. For example, the organisation's management information system should be identified as an asset and should have an IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. Typically, there may be several IAOs within an institution, whose roles may currently be those of e-safety co-ordinator, ICT manager or information management systems manager.

Although we have explicitly identified these roles, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

2.3 Recommended changes

To adequately protect data, organisations may need to make operational and technological changes. Some can be accomplished quickly with existing resources; others will require extra investment and the help of ICT and managed service suppliers. In any given organisation, Information Asset Owners will need to work out the level of change required by carrying out a thorough information risk assessment. Organisations may also need to make staff more aware of data security with training. They may also need to put in place systems and procedures for:

- protectively marking data
- encryption
- audit logging
- responding to security incidents
- secure remote access (using two-factor authentication where needed)
- reviewing contracts for data protection and processing (including cross-border data flows if data is processed abroad)
- reviewing user access requirements for remote access to, and storage of, secured data.

We provide more detailed guidance on these in our good practice guides.

3 Information risk assessment

It is important that organisations conduct thorough risk assessments on the assets they hold. This will help them plan security measures that are practical and proportionate to their specific size and risk profile.

3.1 Conducting an information risk assessment

Organisations should work out criteria for assessing risks. These will need to take into account:

- the assets involved
- legal requirements (such as the Data Protection Act 1998)
- the practicalities of running the organisation day to day
- the impact of incidents on reputation in the community.

Organisations should then identify, describe and prioritise risks against these criteria. The first step in identifying risks is for Information Asset Owners to list information assets that contain personal data or data valuable to the organisation.

Steps in identifying risks include identifying:

- assets
- threats
- existing controls
- vulnerabilities
- consequences.

Once organisations have identified risks they can estimate the size of those risks, that is, the combination of consequence and likelihood.

4 Good practice in information handling

This section gives an overview of our more technical good practice guides. They should help organisations secure data and so reduce the risk of security incidents. They will also help organisations meet the minimum requirements of *Data Handling Procedures in Government*.

4.1 Impact levels and protective marking

The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification.].

4.2 Data encryption

Our *Good practice in information handling: Data encryption* guide explains what data organisations should encrypt. It gives some examples of encryption solutions and information on taking data abroad.
It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

In order to comply with the intent of *Data Handling Procedures in Government*, organisations must take a comprehensive approach to data security. On its own encryption is not enough to secure data. Other important measures include identification, authentication, authorisation, accountability and audit, all of which are explained in detail in the good practice guides.

4.3 Audit logging and incident handling

Good practice in information handling: Audit logging and incident handling gives guidance on how to effectively handle security incidents using audit log data. For example, loss of secured data or breach of an acceptable-use policy (AUP). Audit logging is only valuable if organisations collect the correct log data and store it securely.

Organisations should also collect data in ways that do not overburden systems or make unnecessary work for technicians.

It is a legal requirement of the Data Protection Act 1998 to have a statement of intent that tells staff what kinds of actions are logged or monitored and the level of detail involved.

4.4 Secure remote access

Our *Good practice in information handling: Secure remote access* guide outlines some solutions that organisations can use to allow users secure remote access. It includes using Shibboleth (via the UK Access Management Federation for Education and Research) and Employee Authentication Services (EAS) (via the UK Government Gateway) for two-factor authentication.

The guide also explains how organisations can reduce the need for two-factor authentication by choosing the kind of data that users can access remotely with care. This is particularly important for schools putting in place online reporting to parents, who do not need to use two-factor authentication.

5 Quick wins for data handling compliance

It is recognised that conflicts exist in existing policy, practice, technology and budgets but there are a number of requirements that organisations can implement more easily to reduce the risks of security incidents.

5.1 Operational

- Make sure staff[1] with access to personal data on children or vulnerable adults have enhanced Disclosure and Barring Service (DBS) clearance.
- Read *HMG Security Policy Framework*].
- Appoint a Senior Risk Information Officer (SIRO).
- Identify information assets and for each one, identify an Information Asset Owner.
- Conduct data security training for all users.
- Put in place a policy for reporting, managing and recovering from incidents which put information at risk.
- Shred, pulp or incinerate paper when no longer required.
- Make staff and learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing privacy[2] or fair processing notices[3].

[1] Includes permanent and contract staff within organisations and suppliers.

- Make sure that, where appropriate, contracts for employment state that misuse of such data is a disciplinary matter.

5.2 Technological

- Implement two-factor authentication for all users with access to large data sets, such as all the contents of a management information system.
- Implement and/or require suppliers or hosting partners to implement SSL or IPSec encryption for remote access to personal data in management information systems, learning platforms and portals.
- Encrypt media that contains personal data that is to be removed from the organisation.
- Securely delete and overwrite to government standards all files that contain personal data when no longer required.

6 Additional requirements

After addressing the 'quick wins', organisations should:

6.1 Operational

- Incorporate requirements for managing information risk in HR and contract processes as necessary.
- Ensure all new or changed contracts implement the latest Office of Government Commerce (OGC) security and data protection clauses.
- Ensure that personal data is not exported outside the European Economic Area (EEA) unless EU Model Contracts or Binding Corporate Rules (BCRs) are in place; particular attention is required to be sure your support contractors are fully compliant (note that BCRs require written approval from the Information Commissioner's Office (ICO)). For more information, see the ICO website Conduct privacy impact assessments in accordance with the ICO
- Report significant data protection incidents through the SIRO to the ICO based on the local incident handling policy and communication plan.

6.2 Technological

- Stipulate that suppliers implement encryption and remote access requirements in each application.
- Require suppliers to implement protective markings for any system-printed material that contains personal or sensitive data.
- Put in place an audit logging infrastructure.
- Implement necessary changes to applications to restrict access.

Appendix 2 - Good Practice in Information Handling

Good practice in information handling:
Data security dos and don'ts

We have written this guide for anyone working in a school, college or university who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work. Its aim is to raise your awareness of where potential breaches of security could occur. Following these 'dos and don'ts' will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your organisation may suffer if you lose personal data about individuals.

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

1 Your roles and responsibilities

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

6.3 Important 'dos'

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

6.4 Why protect information?

Organisations hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of your organisation. This can make it more difficult for your organisation to use technology to benefit learners.

6.5 What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

If you don't already know, find out who is acting as your Information Asset Owner.

6.6 Using protective markings

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed.

Your Information Asset Owner should help you work out how you need to mark the information you view as part of your job. There are different levels of marking depending on how just how sensitive the information is.

6.7 Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these ‘dos and don’ts’ will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

6.8 Working online

6.8.1 Do

- make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT team if you need help.
- only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- make sure that you only install software that your IT team has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your IT team.
- check that your organisation has an acceptable-use policy (AUP)[4] for the internet and ensure that you follow it.

6.9 Email and messaging

6.9.1 Do

- read your organisation's email policy
- report any spam or phishing[5] emails to your IT team that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

6.9.2 Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that your IT team has put in place or recommended
- email sensitive information unless you know it is encrypted[6]. Talk to your IT team for advice.
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails.

6.10 Passwords

6.10.1 Do

- follow your organisation's password policy
- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

6.10.2 Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

6.11 Laptops

6.11.1 Do

- shut down your laptop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

6.11.2 Don't

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.

6.12 Sending and sharing

6.12.1 Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

6.12.2 Don't

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

6.13 Working on-site

6.13.1 Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

6.13.2 Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

6.14 Working off-site

6.14.1 Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

7 Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office [http://www.ico.gov.uk].