Name of Policy: Secure Handling and Transit Policy

Date of Policy: May 2018
Review Date: May 2020

Introduction

With multi-site, home and mobile working on the increase we need to be more aware of the limited circumstances in which paper records/hard copy material containing personal or other confidential data may be taken out of, or accessed away from the office. This policy sets out the nature of those limited circumstances and details the security measures that we need to adopt when transporting or storing paper records/hard copy material off site, particularly when such records contain personal or confidential data.

This Policy covers all unencryptable data and includes paper records, photos, 3rd party unencrypted cds/dvds, etc.

These security methods must be robust enough for the type of information in the records. This involves considering in each case:

- The value, sensitivity and confidentiality of the information being taken off-site
- The risk of the information being lost or stolen
- The damage or distress that could be caused to individuals if their personal or other confidential data were to be lost or stolen, and
- The reputational and financial damage that could be caused to the Solent Academies Trust or other agencies or organisations as a result of a breach.

This policy applies to all Trust employees, including placements and temporary staff, agency workers, consultants or third party contractors accessing or using personal or confidential information held by the Trust, or doing so whilst otherwise acting on behalf of the Trust.

Whilst primarily aimed at ensuring compliance with the General Data Protection Regulation 2018 (“GDPR”), the measures in this policy must equally be applied to the transit and storage of other types of confidential information.

Taking paper records/hard copy material off-site
All Trust employees and others covered by the policy, must always consider whether it is necessary to take paper records/hard copy material containing personal data or other confidential information off-site. The reasons for taking such paper records off-site must always be one of necessity and not convenience.

Taking paper records off-site should only happen when it is absolutely essential to do so and there is no alternative method for accessing or recording the information required. Where paper records have to be taken off-site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and where possible, data should be anonymised.

All employees and others covered by the policy are individually responsible for ensuring the adequate protection of information in their possession and ensuring its safe return.

The principles below are to be adopted and adhered to, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off-site:

- There is a presumption against taking personal or other confidential data contained within paper records off-site.
- This material should only be taken off-site when it is a necessity and not a convenience.
- Where data contained within paper records is taken off-site it should be kept to a minimum both in terms of content and duration. Consider how much information is actually required and avoid taking the whole case file unless this is absolutely essential.
- Whilst off-site paper records that are not being actively worked upon, they must be kept secure and stored separately from encrypted portable laptops which given their obvious value, are more likely to be of interest to thieves. This applies to paper records temporarily in the employee's home as well as when the employee is on the move.
- Where paper records are in transit from one location to another, they should be transported in a way that mitigates against the risk of theft or loss and stored in a separate folder away from other valuables, including portable equipment and other electronic devices.

Before taking paper records off-site you must:

- Ensure you are authorised for the purposes of your job role to remove paper documents containing protected information
- Ensure you comply with the minimum standards set out in this policy

If it is determined that it is unavoidable to take paper records off-site, there are many practical actions which can be taken take to minimise the risk of a data loss. For example:

- Do not carry 'loose' paper records as this increases the risk of dropping or losing them and make sure they are safely within a folder or other appropriate container.
- Do not carry paper records in any bag containing valuables, as these are often the primary target for thieves.
- Ensure paper records are not in transit for any longer than is necessary and they are delivered to their destination at the earliest opportunity.
- Ensure paper records are not away from the office for longer than is necessary and return them as soon as possible.
- Do not leave bags or cases containing paper records visible in a car; if it is unavoidable to store paper records in a car, lock them in the boot.
- Do not leave paper records stored in the boot of an unattended vehicle for any longer than is necessary.
- When travelling on public transport ensure that the contents of paper records are not visible

- When travelling on public transport keep the bag/case containing paper records close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of loss or theft.
- Treat paper records as you would your cash. Remember personally identifiable information about individuals is valuable in the wrong hands and if sensitive personal information is compromised the Trust could suffer a heavy fine.
- Ensure confidential paper waste created away from the office environment is securely disposed of using a cross cut shredder or ensure this is safely returned to Trust premises for secure destruction.

Disciplinary action and criminal offences

Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action and even give rise to criminal offences.

Staff Awareness

All employees and others covered by this policy, with access to personal or other confidential data, must be made aware by the line manager, governors or the senior leadership team of the existence of this policy

All new employees must be made aware of the existence of this policy via their induction process.

Employees who consider they have not received adequate training or information, must raise this with their line manager.

Reporting a data loss

Should an incident occur it is important that you contact the Data Protection Officer (DPO) immediately of what information has potentially been lost or stolen. This allows the DPO and their team to properly assess the risks and issues involved and where necessary, to notify of a data breach through the correct channels.

The promptness of reporting is vital in ensuring quick containment of the breach and, where possible, recovery of personal/confidential information. Any delay in reporting is likely to have a detrimental effect on the breach management process.

Everyone in the Multi Academy Trust has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.