The Challenge Academy Trust: Emergency Data Protection Guidance

This policy note outlines the Trust's approach to Data Protection during the current Covid-19 pandemic. It provides advice and guidance for employees to follow in addition to the current TCAT policies, procedures and practices in place including the TCAT GDPR Policy, data breach reporting and compliance with subject access requests.

The aim is to ensure that staff are able to work from home in such a way as to keep data private and confidential

ROLES & RESPONSIBILITES OF MANAGERS & EMPLOYEES

Managers will:

- ensure that employees are aware of and understand this emergency policy and the existing policies and procedures in relation to all aspects of Data Protection;

Employees will:

- ensure that they are aware of and understand this emergency policy and the existing policies and procedures in relation to all aspects of Data Protection;

STAFF WORKING ARRANGEMENTS

It is understood that in the current emergency, with staff working at home and unable to attend their workplace, staff will be accessing pupil/ parental and staff data at home. This may be through IT remote working or as a result of holding physical files and data at their home and they may also be contacting pupils, parents and staff from within their home environment.

Although it can be difficult, staff must ensure that they take as much care as is reasonably practicable to keep data safe and prevent unauthorised people to access the data.

CREATING A SECURE WORK ENVIRONMENT

If possible, identify an area of the home which can be used to set up a 'workspace' and which is recognised by other members of the household as being private to you and your work and where you can keep disturbances to a minimum when you are working. . It is recognised that this will be easier for some people than others.

Wherever a workspace within the home environment is created, ensure that data is kept as secure as possible by: keeping physical files and papers safe when not in use, by either keeping then in a drawer or a cupboard (ideally locked if possible) or if this is not possible store them in closed files where they cannot be read by someone else in the room

- follow the emergency IT policy, ensuring that data on the screen cannot be seen by others when you are working on it
    - keep your own password private on any shared computers
    - use complex passwords to protect access to shared computers
    - ensure that the screen locks automatically when there is no activity
    - always use the remote access systems provided for work activity
    - never leave remote access systems logged on once work has finished

- always use school email systems to communicate with staff, parents and carers and pupils, never your own personal email systems

- when sharing personal data (for pupils and staff) via email with other staff members, delete the emails as soon as you no longer require the information

- when making private and confidential telephone calls to pupils and staff from within the home environment
    - ensure that other members of the household are not able to overhear the conversation
    - if making the phone call from a member of staff's own mobile or home phone, ensure that the number is blocked from recipient if required

SHARING DATA

It is inevitable that in the current emergency situation, information may be shared more widely that it would otherwise be. In all cases where a member of staff is about to share information of any kind, they should ensure that they ask themselves if they should be sharing the data and if they have permission.

For example, private staff emails and telephone numbers are being shared more widely than would otherwise be the case. If you think you need to pass on this sort of information to a third party (even if that third party is another member of staff), please make sure that you have permission first).

DATA BREACH REPORTING

Data breaches need to continue to be reported in exactly the same way as under normal circumstances in accordance with the GDPR Policy. All breaches must be reported to the academy Data Protection Lead in the first instance.

SUBJECT ACCESS REQUESTS

Subject access requests must continue to be responded to in line with the GDPR Policy. All requests must be reported to the academy Data Protection Lead in the first instance.