DATA PROTECTION & CONFIDENTIALITY POLICY AND PROCEDURE

Caremore Group

Issue Date:	1st September 2019
Author:	James Robertson & Kyle Price
Review Date:	1st September 2020
Issue Number:	1

CONTENTS

PURPOSE

This policy is in place to ensure all staff, governors and Trustees are aware of their responsibilities and outlines how the Trust complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Hope Learning Trust York believes that it is good practice to keep clear practical policies, backed up by written procedures.

Caremore Group may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authorities, DfE, other schools and educational bodies, and children's services.

SCOPE

Data protection and confidentiality policy and procedures apply to all workers who encounter personal information including bank, agency and locum staff, students, voluntary staff, contractors and trainees on temporary placements.

Unit Managers are responsible for ensuring awareness of and compliance with this Policy across all areas.

Everyone who handles personal information for or on behalf of Caremore Group is responsible for its safety and security as well as compliance with the Data Protection Act. This includes personal responsibility for notifying Caremore Group once about any security breach or data loss affecting personal information, in line with the Incidents and Accidents Procedure.

The Health and Social Care Act defines 'confidential personal information' as information that "is obtained by Caremore Group in terms or circumstances requiring it to be held in confidence and relates to and identifies an individual".

- Racial or Ethnic origin
- Criminal convictions
- Sexuality.
- Financial details
- Education, training and employment exp

- Physical or mental health.
- Religious beliefs.
- Social or family circumstance

POLICY

It is mandatory that the service users' rights to confidentiality be safeguarded in accordance with the common law duty of confidentiality and Article 8 of the Human Rights Act 1998. The Care service employee will use information only in the best interests of the Service user and where possible with their express consent. All information, verbal, written, electronic or photographic / video / audio recording is managed in line with the Data Protection Act 1998 and The Access to Health Records Act 1990.

PROCEDURE

DATA SECURITY (COLLECTION AND STORAGE)

Staff must ensure all data collected and stored is limited to only that which is vital for the safeguarding and care of the Service user. This relates to personal data and health information essential to establish individual needs and provide staff with the means to plan care and support.

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the Caremore Group enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff may NOT use personal (i.e. owned by the member of staff) laptops, smartphones, computers, tablets, hard drives or other devices for Caremore Group purposes, including accessing school or Caremore Group email accounts and downloading documents. Use of personal devices for school/Caremore Group purposes outside of school premises is also prohibited unless given express permission by a member of senior management.

Caremore Group employees who use personal devices for Caremore Group purposes to access Caremore Group email accounts agree to download or print documents only as necessary; any hard copies of Caremore Group documents must be brought to the office for secure disposal once no longer required. Electronic copies must be securely deleted from any private device including any metadata relating to the document. Emails containing personal data will be deleted once no longer required for the initial purpose.

All necessary employees of Caremore Group are provided with their own secure login and password, and every computer regularly prompts users to change their password.

All Caremore Group employees will be given access to relevant Service user or Caremore Group documents via secure remote access; these documents must be downloaded or printed only as necessary; any hard copies of these documents must be brought to the relevant office for secure disposal. Electronic copies must be securely deleted from any private device including any metadata relating to the document.

Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient. 17 HLTY Data Protection Policy 2018

Circular emails to parents/guardians are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the placement /office premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of Caremore Group containing sensitive information are to be supervised at all times.

The physical security of the Caremore Group's buildings and storage systems, and access to them, is reviewed on a quarterly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Caremore Group takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action

DISCLOSURE

Information and Data should only be shared with those identified as eligible to access it. Information and Data must only be shared for the purposes of safe delivery of care and ensuring individual needs are met. Information and/or Data passed to a care worker may be shared with members of the care team where they are concerned with the care and treatment of the Service user. Staff are required to first confirm the identity and right of access of any third-party seeking information about a Service user or The Agency in writing, by telephone or in person before any disclosure is made.

Prior to the disclosure of any information about the service user, consent should be obtained from the service user and/or service user's social worker. There are many valid reasons informal carers should be informed and involved with the professional care of their loved one. If family members should wish to pass on their concerns or views to a member of care staff this does not constitute a breach of confidentiality by the member of staff.

CONSENT

As far as reasonably practicable, written consent to the use of personal information should be obtained from each service user or their advocate. Inform the subject when gaining consent of the specific details of the information/action to be shared and with whom. This should form part of the information provided at the outset of admission to the service

- Should the Young person lack the mental capacity to consent to information being shared, staff may share information if it is in the Young person's best interests (in accordance with the principles of the Mental Capacity Act 2005). Staff should still clearly explain to the service users the reasons for the decision to share information and accurately record these.

- Should there be any concerns in these areas' advice should be sought from your supervisor.

Access to information, data and records must be managed according to legislation. Service users or their advocates may seek permission to access health information in writing and access must be managed appropriately. It is good practice to involve service users with the collection and recording of personal data as this ensures focus on the needs and rights of each individual.

Unless strict management of information is assured, social media use should be avoided to protect the rights of all individuals in our care. Staff are prohibited from discussing confidential information about service users in any place where third parties might access it, such as in a public place outside of the placement.

Staff are to ensure that all information and data held relates only to the specific service user. Additional care must be taken to limit recording to identify only the Young person whose record it is, and not to include sensitive identifiable data about others in Care Plans and record entries.

Confidentiality with respect to a Service User may only be broken if:

- Information is required by statute or court order.

- Information obtained suggests the service user is at risk of harm to themselves or from others, or others may be at risk of harm from the service user, and where the passing on of information would be in the person's interest, or the wider public interest.

- The young person may have broken any criminal laws where there is justification regarding the public interest to breach confidentiality, Section 115 of the Crime and Disorder Act 1998 gives a power (but not an automatic duty) to organisations to disclose information to the police 'for the prevention, detection and reduction of crime'. This applies in England, Wales and in Scotland (where the Crime and Disorder Act is amended by the Criminal Justice (Scotland) Act 2003).

All breaches of this is policy are punishable in line with the Caremore Group disciplinary and grievance policy.

CCTV AND PHOTOGRAPHY

Caremore Group understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles, as outlined in the company's CCTV & Surveillance Policy.

Caremore Group notifies all service users, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose

All CCTV footage will be kept for three days for security purposes; the Operations Director is responsible for keeping the records secure and allowing access.

Caremore Group will always indicate its intentions for taking photographs of service users and will retrieve permission before publishing them.

If the Caremore Group wishes to use images/video footage of service users in a publication, such as the Caremore Group website, brochure, or recordings of keywork activities or group trips, written permission will be sought for the particular usage from the parent/guardian of the service user

Precautions are taken when publishing photographs of service users, in print, video or on the Caremore Group website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

DISPOSAL OF CONFIDENTIAL INFORMATION

In the event of a service users' death or leaving the service, records should be removed from circulation and retained in secure archive storage. There is a requirement to retain care and clinical records for not less than 3 years in line with Part 3 section 17 of The Care Homes Regulations 2000.

Should confidential information no longer need to be stored, in order to ensure no risk of third parties accessing sensitive data, destruction of paper records must be by shredding. Destruction of electronic records by deletion must be undertaken in a way that ensures no future retrieval is possible.

DBS DATA

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication

SUBJECT ACCESS RIGHTS (SARS)

Individuals have a right to access any personal data relating to them which are held by Caremore Group. Any individual wishing to exercise this right should apply in writing to the Senior management. Any member of staff receiving a SAR should forward this to a member of senior management.

BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Caremore Group shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO

COMPLIANCE

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.