November 2018

Information Security Management Policy

Contents

Objectives of our Policy and Procedures

a) MY Trust holds large amounts of confidential information and places special emphasis on information quality, security and management. It is our policy to make sure that people have no surprises about how information about them is collected, held, used and destroyed. It is also our policy that the information and intellectual property belonging to our organisation is treated with the respect it deserves.

b) It is the responsibility of all our staff, volunteers and Trustees to protect confidential information from inappropriate disclosure and to take every measure to ensure that person identifiable information is not made available to unauthorised persons. This applies to manual and computer records and also conversations about support or interventions with young people and/or staff. We expect this policy and accompanying procedures to become part of the DNA of all our staff, volunteers and Trustees. As such individuals, our partners and our organisation itself should be reassured by our commitment and actions.

c) Our policy and accompanying procedures have two core objectives:

Objective 1: To ensure the information about service users, our staff and volunteers, and the intellectual property of our organisation is treated respectfully and within the law, regulation and stated expectations.

Objective 2: To provide clear, transparent guidance and procedures for our staff and volunteers to manage their work practically in accordance with this policy.

Policy Statement

d) Confidentiality is a cornerstone of practice within MY Trust and the relationship between a member of our staff and a young person depends on it. Young people and families need to be able to tell the truth about deeply personal matters, knowing that this information will not be improperly managed or disclosed. Similarly the relationship between MY Trust as an employer and our staff and volunteers also is one based on trust and confidentiality.

e) People using our services as well as our staff and volunteers deserve a lot more than just information security. Individuals need to know that those responsible for working with them and our organisation more generally collects, manages and shares information

reliably and effectively. Confidential information about an individual must not leak but it may well need to be shared in order to provide a seamless integrated service to a young person/family or effective management and support for an employee.

f) The General Data Protection Regulation (GDPR), 2018 protects individuals against the misuse of personal data and may cover both manual and electronic records. All records held on computer or in manual files fall within the GDPR, unless the data in anonymised.

g) Through this policy, we ensure that personal data is:

- Processed with lawfulness, fairness and transparency
- Is only processed for specific, explicit and legitimate purposes (purpose limitations)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)
- Accurate and where necessary kept up to date (accuracy)
- Kept in a form which permits identification of data subjects for no longer than necessary (storage limitations), and
- Is processed in a manner that ensures appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage (integrity and confidentiality)

h) Through this policy, we ensure that data is processed lawfully under one of these conditions.

a) Consent: the individual has given clear consent to process their data for a specific purpose
b) Contract: the processing is necessary for a contract with the individual, or because they asked us to take specific steps before entering into a contract
c) Legal Obligation: the processing is necessary for us to comply with the law.
d) Vital Interests: the processing is necessary to protect someone's life
e) Public Task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law, or
f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests
g) Special Category Data
h) Criminal Offence Data

i) Through this policy, we ensure that data is only processed following these rights for individuals, depending on the lawful basis for processing.

a) The right to be informed
b) The right to access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object, and
h) Rights in relation to automated decision making and profiling

j) For employment purposes, the most important right is our employees' right to know what personal data is held about them and to have access to it.

k) It is our view that for too long, people have hidden behind the relative obscurity of Data Protection Acts or alleged rules of information governance in order to avoid taking decisions that would benefit service users. Through this policy and procedures we strike

the balance between confidentiality, information security and information sharing to ensure effective support for service users and employment practice.

l) At MY Trust we are equally committed to ensuring that service users' wishes are respected in relation to how their information is used. While people are unlikely to object to sharing confidential information that enables better outcomes for them personally, there may be some who do not want it used for purposes such as research or reshaping services to achieve better services more generally. Our policy and procedures support the individual's right to object and sets out how we will respect this.

m) We will achieve our policy through **Eleven Rules** that provide the thread through all of our work and employment practice.

For all Individuals including Service Users:

- **Rule 1**: Personal information should be treated confidentially and respectfully
- **Rule 2**: Our staff will share confidential information when it is needed for the safe and effective support of an individual
- **Rule 3**: Data used to target prevention and intervention should be robust
- **Rule 4**: Information that is shared for the benefit of the community should be anonymised
- **Rule 5**: Personal Data will be processed lawfully, upholding everyone's rights

For our employees, volunteers and Trustees:

- **Rule 6:** Personal data relating to employees, volunteers and Trustees should be collected, held and shared only where there is a sound business reason
- **Rule 7:** Computer systems, email and internet including personal devices of employees should be used appropriately
- **Rule 8:** Our organisation owns all Intellectual Property and inventions produced by our employees
- **Rule 9**: We have robust practices for our storage, retention and destruction of information
- **Rule 10**: We have rigorous but proportionate accountabilities and monitoring to ensure our rules are followed
- **Rule 11**: Allegations of or actual breaches of data protection or confidentiality will be managed and investigated fairly and promptly

Definitions

n) GDPR Principles

The Regulation requires that personal data:

- Shall be processed fairly and lawfully
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose
- Shall be accurate and where necessary kept up to date
- Shall not be kept longer than is necessary for that purpose
- Processed in accordance with the rights of the data subject
- Appropriate measures are undertaken against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data
- Shall not be transferred to a country or territory outside of the European Economic Area unless that country/territory assures standards of data processing

o) Caldicott Principles

We will apply the six general principles of good practice as follows:

- Justify the purpose
- Do not use person identifiable information unless absolutely necessary
- Use the minimum person identifiable information
- Access to person identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law

p) Confidential Information

Confidential information can be anything that relates to young people, staff, (including volunteers, temporary and agency staff, student placements), their family or friends. It also includes any MY Trust business sensitive information.

Information can take many forms including client records, assessments, letters, emails, texts, faxes, audits, forms, contracts and service agreements, employee records, occupational health records and the like.

Information may be held on MY Trust servers, client databases, computer file or printout, CDs, portable devices such as laptops, tablets, mobile phones, photographs, video/digital cameras and even heard by word of mouth.

q) Personal information

Personal information is information which is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Person identifiable information is anything that contains the means to identify a person (eg, name, address, postcode, date of birth, NI number, IP address). Even a visual image (eg photo) is sufficient to identify an individual.

r) Special Categories of Personal Data

The GDPR refers to sensitive personal data as "special categories of personal data". Special Categories of Personal Data is personal data consisting of information related to:

- Race
- Ethnicity
- Religious or other beliefs
- Political opinions
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992
- Genetics
- Biometrics (when used for ID purposes)
- Health
- Sexual life
- Sexual orientation

Certain categories of information are legally defined as personally sensitive and should be most carefully protected by additional requirements stated in legislation (eg; information regarding sexually transmitted diseases, HIV, transgender procedures and termination of pregnancy).

s) Processing

The term 'processing' is used within the GDPR. It applies to a range of activities including the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

t) Verification and Vetting

'Verification' covers the process of checking that details supplied by job applicants (eg qualifications) are accurate and complete. Verification therefore is limited to checking of information that is sought in a job application or provided by an applicant; this includes taking up references and the use of verification through the Disclosure & Barring Service. Vetting covers any activity we undertake to make our own enquiries from a third party about a job applicant's background and circumstances. It goes beyond the verification of details as per para (v) above. The para reference seems to be incorrect -it is v below or 5 or another?

Legislative and Regulatory Basis

u) Our policy fits with and is compliant with the following legislation and regulation:

- Common Law (Duty of Confidence)
- General Data Protection Regulation, 2018
- Human Rights Act 1998 (Article 8)
- Freedom of Information Act 2000
- Children Act 2004 Sections 10 & 11
- Education and Inspections Act 2006
- Criminal Justice Act 2003 (Section 325(4))
- Crime and Disorder Act 1998 (Section 115)
- Professional Performance Act 1995
- Mental Health Acts 1983 & 2007
- Mental Capacity Act 2005
- Regulation of Investigatory Powers Act 2000
- Equality Act 2010
- Working Together to Safeguard Children (2018)
- Kent & Medway Safeguarding Children Procedures
- MAPPA Guidance 2009
- Civil Contingencies Act 2004
- Learning and Skills Act 2000 (as amended)
- Computer Misuse act 1990
- Justice and Coroner's act

v) Our policy fits with practice guidance from the Information Commissioner's Office (ICO) and the Kent & Medway Information Governance Protocols.

RULE 1	**Personal information should be treated confidentially and respectfully**

1. Underpinning law and professional practice are basic issues of right and wrong; it is right to respect people's privacy and wrong to betray their confidences. Prying and gossiping are unethical.

Maintaining trust should always be a priority

2. The duty of confidentiality is based on trust and respect and this is fundamental to safe, effective services. An environment of trust encourages people to be open and honest and to provide all the details necessary so they receive the best support and services possible. People need to trust that their confidential information is safe when confiding in or sharing information with any of our staff or volunteers.

3. In the unlikely event that confidential information about an individual is inappropriately disclosed, the individual should receive an explanation and an apology from the individual and/ or from our organisation.

To retain an individual's trust and to support effective practice, our database record should be as complete as possible, accurate and fit for purpose

4. We maintain a number of confidential databases with many linked to service delivery contracts. A key part of the trust relationship is ensuring that our database record for a individual (including flagged fields, assessments, documents and communications from other agencies) is complete, accurate and fit for purpose. Information is not safe if it is not accurate and support for a service user is less effective if the information is not accurate. It is the responsibility of each member of our staff to ensure this.

5. Our staff may note personal information on paper to ensure accuracy of recording and is less intrusive than typing. Such handwritten notes should be typed into or scanned into the relevant database within one week and the handwritten notes destroyed securely.

6. Our staff may temporarily store personal information on MY Trust's MS Office 365 One Drive or on their PC for use during an activity. This information will be obtained from the relevant database to ensure accuracy, the database will still be updated accordingly if any new information is gathered. These electronic documents will be deleted when no longer needed.

7. Sometimes it's necessary to use personal devices to access information, staff will agree to and sign the Bring Your Own Device – Acceptable Use Policy if they wish to do this.

Confidential information should always be respected and maintained

8. Information must never be discussed in public, or via the open internet – for example social media and professional forums.

9. Information will be shared within our staff teams and with management as part of ensuring the effective support for the service user and our staff. Staff must however be

vigilant that service user information is not overheard by those who do not have a legitimate need to know (including other young people, visitors and staff who do not need to be involved). Face to face and mobile telephone conversations present particular risk in the following areas:

- Public areas of our own or other agencies' centres
- Stairwells
- Toilets
- Public transport
- Public spaces including streets, shops, cafes, pubs and restaurants

10. Information will be protected and used securely within our offices through the following procedures:

- Confidential papers will not be left on desks or in unsecured cabinets when the office is 'unstaffed'.
- We will log out of a database when leaving a computer unattended
- Staff will wear identity badges at all times
- Visitors will be signed in, wear visitor badges and as necessary escorted within an MYT building
- Codes for security systems (including alarms or keypad locks) or security system procedures must be kept confidential. Any suspected breaches or attempted breaches must be reported immediately to the Chief Executive.
- Confidential waste must not be used as scrap paper and personal information must be disposed of by shredding or using the appropriate secure waste collection facility.

11. For all types of records, staff working in facilities where records may be seen must:

11.1. Shut/lock doors and cabinets as required
11.2. Wear ID badges
11.3. Query the status of strangers – especially if in and around secure areas
11.4. Tell line manager or alternative person in authority of anything suspicious or worrying
11.5. Not tell unauthorised personnel how the security systems operate
11.6. Not breach security themselves

Abuse of privilege

12 It is strictly forbidden for an employee or volunteer to look at any information relating to their own family, friends or acquaintances unless they are directly involved in the young person's intervention and the line manager has given prior authorisation. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action. If any member of staff or volunteer has concerns about this s/he should discuss it with their line manager.

RULE 2	**Our staff should share confidential information when it is needed for the safe and effective support of an individual**

1. Confidential information should be shared within the direct staff team and management within our organisation as this will result in better support and service from us. Information should be shared with those in our staff who 'need to know' and not as part of gossip.

2. Sometimes individuals are put at risk when confidential information is not shared. Tragically, lives are put at risk when information has not been shared and this has been identified as a root cause of failure in many serious case reviews. Our safeguarding policies and procedures cover information sharing in this instance and exercising professional curiosity is necessary and often requires discussing confidential information with a colleague or manager.

3. It is paramount that confidential information is shared securely and in compliance with rule 1 of this policy.

4. **Specific instructions for confidential information via email**:

   4.1. Add the words 'Private and Confidential' in the subject heading of the email. Never put any person identifiable details (definition in paragraph P on page 5) in the subject line.
   4.2. Request a delivery/read receipt when sending the email
   4.3. Only the following email accounts are approved as standard for transfer of person identifiable information outside of the organisation:

   - @cjsm.net Criminal Justice Secure Network
   - @gsi.gov.uk Government Secure Network
   - @nhs.net Government Secure Network
   - @gsx.gov.uk Government Secure Network
   - @gsisup.co.uk Government Secure Network
   - @pnn.gov.uk Police National Network
   - @pnn.police.uk Police National Network
   - @scn.gov.uk Police National Network
   - @psops.net Police National Network
   - @eu-admin.net European Union Secure Network

   - Identity-based encrypted (IBE) emails including ESCC Secure Mail or Egress.

   If there is a need or request to send confidential information by email to an email account not on this list, advice should be sought from management or Impact & Intelligence Officer.

5. We are currently exploring the potential for use of Egress for transferring confidential information and this review will be completed during 2018.

6. The email (and any attachments) should contain the minimum information required, removing person identifiable details wherever possible.

7. Once the email is confirmed as received, it should be added to the young person's record in the relevant database, deleted from the Sent items folder in your account and then deleted from the Deleted Items folder.

8. **Specific instructions for receiving**:

   8.1. Ensure that receipt of the email is acknowledged
   8.2. The email and attachments must be saved to a suitable (access controlled) network drive, where it can be accessed by appropriate individuals.
   8.3. Emails should not be kept in Outlook for any longer than is necessary

9. Any correspondence referring to a young person must have a copy stored on their electronic client record.

RULE 3	**Data used to target prevention and intervention should be robust**

1 Segmentation is the practice of dividing our target cohorts into groups of individuals that are similar in specific ways relevant to our work, such as age, gender, residency, academic level, interests, habits and the like. Using segmentation allows MY Trust to measure their impact, target groups more effectively and allocate resources to best effect; the UK Government Cabinet Office states

"There is a significant opportunity for local government to improve its performance through more effective use of customer intelligence. Customer information is an under utilised resource at the moment and its value as an 'asset' that can be used to drive improvements to service and performance is not sufficiently recognised by local government. There is increasing pressure for authorities to demonstrate that they can pro-actively identify customer needs and demonstrate how those needs are being met. Measuring performance in terms of impact on customers and their views will become an increasingly important feature of performance management. It is unlikely that the council of the future will be regarded as performing well unless it is using customer information to drive and measure performance. Furthermore, low or reduced grant funding for local authorities together with likely council tax caps over the medium term requires authorities to think about prioritising services and methods of service delivery. It will be hard to do this effectively and even harder to justify without reference to hard data about customers' use of services and their preferences."

2 Young people and other citizens may be segmented by a myriad of different characteristics including for example age, ethnicity, gender, academic attainment or achievement, level of affluence and health.

3 Our information has two types:

- Explicit – database records of who is currently using or has used our services
- Implicit – knowledge of our staff or partner services who are dealing with young people in delivering services.

4. We will try to stick to information that is relevant to a particular business or service effectiveness question; we do not want to make analysis too complex and time and resource consuming but more important we want to avoid trespassing on people's privacy. While most young people will be happy for MY Trust to carry out anonymised profiling work if it means they get a better and more effective service approach this should be limited to what is needed.

5. We will consider privacy and data protection issues carefully when comparing or combining information. Where possible we will make it clear that we will be using information for this reason when we collect it and will gain consent.

6. The key thing with all information to be used in any of our profiling is that it should be as "clean" as possible. We will avoid records that have lots of incomplete or inaccurate data and hence we will maintain our emphasis on data quality through its accuracy, completeness and timeliness.

RULE	4	Information that we share for the benefit of the community should be anonymised

1. One way that MY Trust can support young people and the community is by helping local authorities and other service/education providers plan and resource their own programmes in response to need. We also have contractual responsibilities to share information with contract Commissioners and funders.

2. The GDPR only covers information which relates to a living individual who can be identified from that data, and therefore the same considerations do not apply to anonymised data. However whilst we take seriously our responsibility to inform and influence the wider range of services for young people, we will ensure we do it safely.

3. We share anonymised information in different ways including data bulletins, graphs and charts, headline data figures and dashboards.

4. Prior to publication of any anonymised or aggregated data reports we will ensure that there is no risk of identification of any individual. Such risk may occur when there is a low number of young people in a particularly category being reported or when geographical based reports are published.

RULE 5	**Personal Data will be processed lawfully, upholding everyone's rights**

1 Privacy Impact Assessments have been completed on all contracts and business process to identify the privacy risks in processing individuals' data. These risks have been assessed and minimised proportionately to the need of the processing. Information mapping has been completed to ensure we know exactly what data is being processed and in what form. Staff are trained in understanding this mapping and only process data within the confines of the assessments.

2 The lawful basis for processing has been identified for all of MY Trust's contracts and business processes where individuals' data is to be processed.

3 We will use an organisational Privacy Notice in our work with young people and staff, and each contract and business process will have its own additional Privacy Notice, specific to the data being processed. This explains whether MY Trust acts as Data Controller or Data Processor when delivering contracts for other organisations and what the lawful basis for processing is.

4 The Privacy Notice explains how we look after and treat individuals' information and why and with whom it is shared. The Notice which is written in audience friendly language also advises individuals on how to get in touch with MY Trust to ask questions about their data and to implement their rights under paragraph i of this policy.

5 The Privacy Notice will outline to the individual exactly where their data will be stored, how and for how long it will be kept.

6 All Privacy Impact Assessments, Legitimate Interest Assessments and Privacy Notices are stored in a folder in the MY Trust's Office 365 One Drive and are available for all to view.

7 All Privacy Notices will be available to view and download on MY Trust's website www.themytrust.org

8 All Privacy Notices will be reviewed annually. Each time a new contract is awarded a Privacy Impact Assessment, Privacy Notice will be completed and relevant database adapted to be fit for purpose before the contract starts.

9 Staff are trained on how to identify a Subject Access Request or a Freedom of Information Request and how to manage it. This is outlined in a separate Policy.

10 Data sharing agreements have been updated to ensure GDPR compliancy. MY Trust will continue to be a signatory of The Kent & Medway Information Sharing Agreement and only share Information under these guidelines.

RULE 6	**Personal data relating to employees, volunteers and Trustees should be collected, held and shared only where there is a sound business reason**

Recruitment

1 MY Trust has safe recruitment procedures for paid and volunteer staff (Ref: Safeguarding Children & Young People Policy and Procedures) and the GDPR does not inhibit us from recruiting staff safely or effectively. What it does is help strike a balance between our need as an employer for information and an applicant's right to respect for their private life. The Regulation requires openness and so therefore applicants should be aware what information about them is being collected and what it will be used for. Our approach is to:

- Identify our organisation properly in all adverts so that people know who they are applying to. From time to time we might use a recruitment agency in which case we will make sure that the agency identifies itself and it is made clear that MY Trust are the ultimate employer.
- Collect only information we need for selection and for monitoring the effectiveness of our recruitment advertisements. We will only add an applicant's name to for example our marketing list if they request or agree to receive additional communications from us.
- Be clear about what documents (e.g. passport, visa, exam certificates) we wish to see to verify the information a person provides.
- Ensure that those involved in recruitment and selection are aware that data protection rules apply and that they must handle personal information with respect.
- Collect only information such as banking details from the person that we go on to appoint.
- Only ask for information about criminal convictions if this is justified by the type of job or role we are recruiting for. We will only ask for 'spent' convictions if the job or role is covered by the Exceptions Order to the Rehabilitation of Offenders Act 1974.
- Only verify criminal conviction information by obtaining confirmation via the Disclosure and Barring Service (DBS). We make sure that we are entitled to receive this information and that we follow the DBS process strictly.

2. We may collect sensitive personal information at the point of recruitment to help monitor equality and diversity, for example about applicants' disabilities, race and sexuality. We will keep this information separate from the actual job/voluntary role application and only use the information for the purposes of monitoring access to employment opportunities at our organisation. We provide applicants with opportunity to provide this as anonymised information.

3. We will retain, store and destroy recruitment information in line with Rule 9.

B. Employment Records

4. MY Trust collects, maintains and uses information about our employees and volunteers. In doing this we strike a balance between our need to keep records as a good employer and our staff's right to respect for their private life. The GDPR requires openness and so through Rule 6 of our policy we set out clearly for our employees, volunteers and Trustees what information about them is kept and what it will be used for. We ensure that those who have access to employment records are aware that data protection rules apply and that personal information must be handled with respect.

5. We will keep all employment records secure. Our paper records will be kept under lock and key and password protection will be applied to the relevant database. We will keep each individual's paper records in different tabbed sections within a file to enable those accessing the file to go straight to relevant section rather than peruse all its contents. Only staff with proper authorisation and the necessary training will have access to employment records.

6. Authorised staff accessing the HR records will be expected to record on a log the file accessed, the date and reason. If there is reason for an employee file to be taken off-site, this will need authorisation from the Chief Executive; such authorisation will be shown by signature on this log.

7. We want to be careful about what records are kept about our staff and volunteers and we are determined not to keep information that is irrelevant, excessive or out of date. We will delete information that we have no genuine business need for or a legal duty to keep. It is our policy to make sure that people have no surprises about how information about them is collected, held, used and destroyed and so we will review our employment records in January each year also giving each member of staff the opportunity to review their file with us. Involving staff in this way will allow any mistakes to be corrected and information kept up to date.

8. Data protection does not stand in the way where we are legally obliged to disclose information about our staff; for example, informing the Inland Revenue about payments to our staff or assisting a Police investigation. We will be careful when disclosing any information in the employment record of an employee or volunteer. We will be vigilant to the fact that the person asking for information about our staff may not actually be who they claim to be. We will only disclose if we are satisfied that it is fair to do so; fairness to our staff is our first consideration.

9. Through this policy we recognise the difference between a reference provided in a personal capacity and one given in a corporate capacity. A corporate reference is provided on MY Trust's behalf by one of our staff and only members of the senior leadership team are authorised to provide such references. It is our policy to confirm factual information in a reference: such as dates of employment and posts held, number of days absent through sickness, disciplinary and grievance, safeguarding issues and any other information which we are legally required to provide. We will not usually provide a subjective reference or provide confidential information about a member of staff or volunteer. Our organisation does have a commitment to safeguarding and under legislation including responsibilities through the Disclosure and Barring Service to pass on information about individual employees or volunteers. If we have any doubt we will ask the individual concerned. Employees do not have right of access to a confidential corporate reference from MY Trust but can make access request of the new employer.

10. A personal reference is one given by a member of staff in an individual capacity. It may refer to work undertaken but is not the responsibility of our organisation.

11. We will retain, store and destroy employment records in line with Rule 9.

C. Employee's health

12. In this policy we distinguish between records that include 'sensitive data' and those that do not. The 'sickness record' is used to describe a record which contains details of the illness or condition responsible for an employee's absence. Similarly an injury record is a record which contains details of the injury suffered. The term 'absence record' is used to describe a record that may give the reason for absence as 'sickness' or 'accident' but does not include any reference to specific medical conditions. Our use of sickness and injury records therefore is likely to include sensitive personal data.

13. We might also collect information about employees to administer necessary adjustments to work under the terms of the Equality Act or Occupational Health. We will only use this information for the purpose in which it was collected. We will make sure that the employees know what information has been collected and used.

14. Where possible we will keep sickness records containing details of an employee's illness or medical condition separate from other less sensitive information. We will do this by keeping the sickness record in a sealed envelope in the employee's file.

15. Our accident, incident and near miss records are retained in the secure employee records cupboard and separate instruction is provided to all staff on completing these forms in a way that protects privacy.

D. Pension schemes and Payroll

16. We collect information about employees to administer a pension and death in service insurance scheme. We will not use information required by a third party for general employment purposes.

17. Our annual audit and review of the implementation of this policy will include review of the information provided to a third party and risk of leak to general employment purposes.

18. When an employee joins an MYT pension or insurance scheme we will make it clear what if any information is passed between the scheme controller and our organisation and how it will be used.

19. We ensure all payroll records only retain information which is required legally to pay employees and make relevant contributions to statutory agencies. All records are securely stored in electronic systems and are password protected, with access restricted to only those staff who are responsible for processing payroll.

E. Disclosure requests

20. From time to time third party organisations may request personal information about our employees. In some cases we will be under a legal obligation to disclose and the GDPR

does not prevent this; for example criminal or tax investigations. In other cases we will wherever possible seek the agreement of the affected employee unless we are satisfied that despite the duty of confidence we have to our staff the employee's or wider public interest justifies disclosure. Where a disclosure is requested in an emergency we will make a careful decision as to whether to disclose, considering the nature of the information being requested and the likely impact on the individual of not providing it.

21. Some people will use deception to gain access to personal information or sensitive information about our staff. We will check the legitimacy of any request and the identity and authority of the person making it.

22. Where a disclosure involves the transfer of information about an employee to a country outside of the European Economic Area (EEA) we will ensure there is proper legal basis for making the transfer.

23. As a general rule for staff, disclosure should only happen from a member of the senior leadership team or with the authority of someone within that team. A record of non-regular disclosure will be kept in the employee's HR folder.

24. Within some of our delivery contracts we may be required by Commissioners or funders to share information about our staff; this might include for example DBS numbers and issue dates, qualification levels. In a TUPE situation within a contract tender/renewal, we may be required to disclose information about employees; such information will be anonymised until it is known that employees will be transferred and a separate process will follow. Confirmation will be secured from any recipient organisation (either direct or via the Commissioner) that the employee information will be treated in confidence, used solely for evaluation of the assets and liabilities for the contract or merger, not disclosed to any third parties and destroyed after use.

F. <u>Discipline, grievance and dismissal</u>

25. We are very clear that the Data Protection Act applies to personal information processed in relation to discipline; grievance and dismissal proceedings and our procedures are compliant in this respect. Our managers will maintain the following practice:

- Those involved in investigating disciplinary or grievances should not gather information by deception
- Records used in the course of any proceedings should be of good enough quality to support any conclusion drawn from them
- All records will be kept securely
- Unsubstantiated allegations should be removed unless there are exceptional reasons for retaining them
- We will not access or use information kept about our employees merely because it might have some relevance if it is incompatible with the purpose(s) we obtained it for or is disproportionate to the seriousness of the matter under investigation. In short, those carrying out an investigation do not have unrestricted right of access to information held about the employee under investigation.

26. We will ensure that when employment is terminated that the reason will be shown clearly on the file.

RULE 7	**Our computer systems, email and internet including personal devices of employees should be used appropriately**

1 To maximise the benefits of our computer resources and minimise potential liability, our employees are only permitted to use the company's computer systems in accordance with this policy.

A. General Rules

2 The Company's computer systems, software and their contents belong to MY Trust and they are intended for business purposes. Our employees are permitted to use the systems to assist in performing their work.

3 Under Rule 10 we retain the right to monitor and access all aspects of our systems, including data which is stored on the company's computer systems in compliance with the GDPR, 2018.

4 Our employees should receive prior approval from management before using any part of the computer systems for personal use.

B. Security

5 We require our employees to log on to our computer systems using their own password which much be kept secret. Our employees should select a password that is not easily broken (e.g.; not their surnames). Each employee is responsible for this.

6 Our employees are not permitted to use another employee's password to log on to the computer system, whether or not they have that employee's permission. If an employee logs onto the computer system using another employee's password, s/he will be liable to disciplinary action up to and including summary dismissal for gross misconduct. Any employee who discloses his/her password to another employee will be liable for disciplinary action.

7 To safeguard our computer from viruses, our employees are not permitted to load or run unauthorised games or software, or to open documents or communications from unknown origins. We install anti-virus software on all our devices.

8 We reserve the right to require our employees to hand over all company data held in computer usable format.

C. Use of email

9 Emails can be the subject of legal action (for example, claims of defamation, breach of confidentiality or breach of contract) against both an employee who sent them or MY Trust. Through this policy, our staff are reminded that email messages may be disclosed to any person mentioned in them. Our staff must therefore be very careful if they write about people in emails.

10 Our email facility is intended to promote effective communications relating to our business. Our staff should only use the email system for this purpose. Emails should be written in accordance with MY Trust's Communications Standards and the content and language used in the message should be consistent with best practice. Messages should only be directed to relevant individuals on a need to know basis.

11 Monitoring will take place in accordance with Rule 10.

D. Use of email to exchange confidential information

12 **Specific instructions for sending**:

12.1 Add the words 'Private and Confidential' in the subject heading of the email. Never put any person identifiable details (definition in paragraph P on page 5) in the subject line.

12.2 Request a delivery/read receipt when sending the email

12.3 Only the following email accounts are approved as standard for transfer of person identifiable information outside of the organisation:

- @cjsm.net Criminal Justice Secure Network
- @gsi.gov.uk Government Secure Network
- @nhs.net Government Secure Network
- @gsx.gov.uk Government Secure Network
- @gsisup.co.uk Government Secure Network
- @pnn.gov.uk Police National Network
- @pnn.police.uk Police National Network
- @scn.gov.uk Police National Network
- @psops.net Police National Network
- @eu-admin.net European Union Secure Network

- Identity-based encrypted (IBE) emails including ESCC Secure Mail or Egress.

If there is a need or request to send confidential information by email to an email account not on this list, advice should be sought from management or Impact & Intelligence Officer.

12.4 We are currently exploring the potential for use of Egress for transferring confidential information and this review will be completed during 2018.

12.5 The email (and any attachments) should contain the minimum information required, removing person identifiable details wherever possible.

12.6 Once the email is confirmed as received, it should be added to the young person's record in the relevant database, deleted from the Sent items folder in your account and then deleted from the Deleted Items folder.

12.7 **Specific instructions for receiving**:

12.7.1 Ensure that receipt of the email is acknowledged

12.7.2 The email and attachments must be saved to a suitable (access controlled) network drive, where it can be accessed by appropriate individuals.

12.7.3 Emails should not be kept in Outlook for any longer than is necessary

12.8 Any correspondence referring to a young person must have a copy stored on their electronic client record

13 Inappropriate use

13.1 Misuse of MY Trust's computer systems may result in disciplinary action up to and including summary dismissal. To provide practical guidance for our staff, examples of misuse include but are not limited to the following:

- Sending, receiving, downloading, displaying or disseminating material that insults, causes offence or harasses others.
- Accessing pornographic, racist or other inappropriate or unlawful materials.
- Engaging in gambling.
- Securing loans.
- Forwarding electronic chain letters or similar material.
- Downloading or disseminating copyright materials.
- Not securely and confidentially transmitting confidential information about MY Trust, staff, service users, partners, commissioners/funders, customers/potential customers.
- Downloading or playing computer games.
- Copying or downloading software without authorisation.

RULE 8	**Our organisation owns all Intellectual Property and inventions produced by our employees**

1. Rule 8 is covered through specific statements in each of our employee's employment contract. These statements are repeated below in paragraphs 8.2 and 8.3.

A. Employment contract - Confidentiality:

2. Our employees acknowledge that during the course of their employment they will have access to Confidential Information belonging to the Company. Our employees shall not at any time during (except in the proper course of carrying out their duties) or after their employment whether directly or indirectly disclose to a third party or make use of any Confidential Information. For the purposes of this section, "Confidential Information" shall include: information relating to the Company's clients and prospective clients; business methods; corporate plans; finances; business opportunities and development projects of the Company; trade secrets including designs or inventions belonging to the Company; all or any information relating to the marketing or sales of any past, present or projected product or service of the Company; and any information in respect of which the Company owes an obligation of confidentiality to a third party.

B. Employment Contract – Intellectual Property.

3. The Company will own all Intellectual Property and Inventions that our employees produce in the course of their employment duties absolutely. Our employees agree to sign all documents and carry out all such acts as will be necessary to achieve this. Our employees also waive all moral rights in all work for which the copyright is owned by the Company or will be owned by the Company, further to this section. For the purposes of this section, "Intellectual Property and Inventions" means patents, trademarks, service marks, registered designs (including application for and right to apply for any of them) unregistered design rights, trademarks or service marks, trade or business names, copyright, or know how and any similar rights in any jurisdiction. Rights and obligations under this section in respect of Intellectual Property made during our employees' employment shall continue in force after termination of their employment howsoever caused and will be binding upon your representatives.

4. From time to time we may employ people under employment contracts issued by other organisations (e.g. staff transferred to MY Trust under Transfer of Undertakings (Protection of Employment) Regulations (TUPE)). In this instance, paragraphs 8.2 and 8.3 above will apply under the overall commitment of this policy.

RULE 9	**We have robust practices for our storage, retention and destruction of information**

1 Our Retention & Disposal Schedules held in a separate document provide staff with guidelines for the retention of documentation. The schedules are structured around legislative requirements and guidelines issued by a range of bodies and statutory guidance including:

- Information Commissioner's Office
- Chartered Institute of Personnel and Development
- Charity Commission
- Companies House
- Health & Safety Executive
- NSPCC
- Buzzacott Accountants
- Working Together to Safeguard Children 2018

In addition, common practice amongst local authorities has also been used.

2. Some documents need not be retained and will be routinely destroyed in the course of day to day business. Such documents are unimportant and only of short term use i.e., incidental phone messages, working notes and the like.

3. To securely remove information from electronic media, it must be overwritten. The more times it is overwritten the harder it is to recover. Your line manager and/or Impact & Intelligence Officer should always be consulted.

4. Confidential waste bins and shredding machines will be available to destroy paper documents in all MY Trust buildings.

5. The retention schedules set practical guidance for our staff and volunteers on:

- Information to retain
- how and where to retain it, and
- when and how to destroy it

6 To assist, they are divided in to broad areas relevant to MY Trust's operations and service delivery. The schedules are subject to annual review but are likely to be updated mid-year in response to new information, policy, precedent and legislation.

RULE 10	**We have rigorous but proportionate accountabilities and monitoring to ensure our rules are followed**

A. Accountabilities

1 We will ensure that our organisation has embedded a culture of safe management of data and information and that our staff are clear about this in all that we do. MY Trust is registered with the Information Commissioners Office.

2 The Chief Executive has overall responsibility to the Board of Trustees for ensuring our policy is implemented and for promoting data protection and secure collection, use and retention of information in all aspects of our operation and service delivery. S/he will be competent in data protection matters.

3 The Chief Executive cannot delegate the overall responsibility for the implementation of this policy but can delegate to the senior leadership team and the Impact & Intelligence Officer some of the operational aspects of its implementation.

4 MY Trust has a clear line management structure which includes responsibilities for ensuring quality of service delivery. Information security is a responsibility shared by all and as such all our staff, volunteers and Trustees will work within the eleven Rules of this policy. Employees and volunteers are accountable for information security practices through this line management structure.

5 All staff and volunteers will be trained to understand and act appropriately with information security. MY Trust will provide support to staff through the provision of a robust induction, training, supervision and appraisal programme. In addition, staff can access support and guidance from line managers.

6 Staff are expected to attend initial and refresher information security training as appropriate. Where our services are contracted to other agencies it is the responsibility of the contract manager to ensure appropriate information security arrangements are in place.

7 All concerns or allegations of abuse and neglect will be reviewed. Staff are encouraged to raise concerns in a spirit of openness and transparency but also have the Whistleblowing Policy as a route to raise any concerns.

B. Data Protection Audits

8 We may undertake periodic announced and unannounced audits of the implementation of the eleven Rules. Such Audits may be led by any member of the Senior Leadership Team, the Impact & Intelligence Officer, a Trustee or an external expert.

9 Further as part of the review cycle for this policy and rules we will undertake a deeper audit of data protection and information security on an annual basis. The Annual Audit will be led by the Chief Executive and supported by the Impact & Intelligence Officer. The annual Audit results will be reported to the Board of Trustees and will cover:

- This Policy and procedures
- The information being gathered, retained and destroyed
- The understanding of Senior Leadership Team and all staff and volunteers.

10 We will use the annual audit to remind staff and volunteers of the extent to which individuals and the organisation can be liable if they knowingly or recklessly disclose personal data in contravention of these policies and procedures.

RULE	11	**Allegations of or actual breaches of data protection or confidentiality will be managed and investigated fairly and promptly**

1 Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. MY Trust also has measures against breaches of confidentiality or trust. Rule 11 of this policy is one of our measures.

2 A breach of data security or confidentiality can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained through deception.

3 However the breach has occurred, we have four important elements to breach management:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

A. <u>Containment and Recovery</u>

4 Data or confidentiality breaches will require not just an initial response to investigate and contain the situation but also recovery and where necessary damage limitation. To achieve this we may involve input from specialists including IT, HR and legal and in some cases contact with external stakeholders and suppliers.

5 Where a breach is alleged or known we will do the following:

- Name the lead for investigating the breach and ensure s/he has the appropriate resources
- Establish who needs to be made aware of the breach and inform them what they are expected to do to contain the breach
- Establish whether there is anything we can do to recover any losses and/or limit the damage the breach can cause.
- Inform the ICO
- Where appropriate, we will inform the Police.

B. <u>Assessing the risks</u>

6 Some data and confidentiality breaches will not lead to risks beyond inconvenience to those who need the data to do their job (e.g. an irreparable laptop). Other risks might include theft of data which could then be used to commit identity fraud or gain inappropriate access to children and young people. Risk of confidential material and intellectual property could lead to MY Trust suffering financial and reputational risk. We

will therefore assess the risks that might be associated with the breach before deciding on what steps are necessary for immediate containment.

7 We will consider the following points when making this assessment. These points are illustrative rather than a definitive list.

- What type of data is involved?
- How sensitive is it? We will consider whether it is sensitive because of its personal nature (e.g. looked after children status) or because of what might happen if it is misused (e.g. address, bank account details).
- If data has been lost, are there any encryptions or other protections?
- What has happened to the data? Has it been stolen, lost or damaged?
- What could the date tell a third party about the individual?
- How many individuals' personal data are affected?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals? Are there risks to physical safety or reputation, or a financial loss or a combination of these or other aspects of their life?
- Are there wider consequences such as risk to public health, loss of confidence in MY Trust?
- If confidential or commercially sensitive material is involved, how might it be used and what might the impact be to MY Trust or our commissioners, partners and customers?

C. <u>Notification of breaches</u>

8 Informing people and organisations that there has been a data security breach is an important element in our breach management strategy. However, we understand that informing people is not an end in itself. Our notification will have a clear purpose usually with one or more of the following reasons:

- Enable the affected party or individuals to protect itself/themselves
- Allow the appropriate regulatory bodies to perform their functions
- Contractual requirement with relevant Commissioners
- Provide advice
- Deal with complaints

9 When notifying those affected, we will:

- Include a description of how and when the breach occurred and what data was involved.
- Include details of what we have already done to respond to the risks posed by the breach
- Give clear advice on the steps they can take to protect themselves and also what MYT is willing to do to help them
- Provide a way for the affected individual to make contact with MYT further information or to ask questions

10 The Chief Executive will notify the Information Commissioner, we will follow the ICO guidance on notification.

10.1All data breaches, however small or large will be formally notified to the Board of Trustees.

D. Evaluation and response

11 We will evaluate the effectiveness of our response to any breach or alleged breach to ensure that the risk of repeated breach is minimised and any learning is shared. Such evaluation may lead to one or more of the following:

- Staff training – individual or collectively
- Briefings about expected and good practice
- Revision to this policy and procedures
- Consultation to revise employment contracts

E. Disciplinary procedure

12 Breaches of data and/or confidentiality will be investigated and may result in disciplinary investigation. A disciplinary investigation will follow the procedures set out in the disciplinary policy and may commence during a data/confidentiality breach investigation or following it.

13 Investigations to breaches of data and/or confidentiality involving Trustees, staff or volunteers no longer involved with MY Trust will continue as if they were still involved. We understand that the range of disciplinary measures available to the organisation are different if the person or persons involved are no longer involved and in this instance legal advice will influence the action taken.

Information Security Management Policy
Retention and Disposal Schedules

Schedule	Contents of retention
A	Applicants for employment
B	Employee HR records
C	Governance records
D	Health & Safety records
E	Accounting records
F	Buildings and plant
G	Insurances
H	Service delivery – Partnerships
I	Safeguarding, child protection, children in need, children looked after
J	General service delivery – service user's records

Schedule A: **Applicants for employment**
Best practice guidance from Information Commissioner's Office and Chartered Institute for Personnel Development

	Information	**Storage**	**Retention Period**	**Destruction method**	**Reason and/or Notes**
A1	Electronic applications for unsuccessful applicants.	Email accounts	1 week from interview date; Print hard copies and follow A2 below	Delete from Inbox, Sent box and Trash folders	Equality Act 2010, Limitations Act
A2	Applications from and interview notes for unsuccessful applicants	Locked cupboard, folder labelled with interview date & advertised post/electronic systems password protected	6 months	Confidential waste or shredding	Equality Act 2010, Limitations Act
A3	Unsuccessful applicants' contact information	Locked cupboard/ electronic systems password protected	12 months	Confidential waste or shredding	MYT business need
A4	Vetting information	Interviews folder and/or Employee HR file/ electronic systems password protected	12 months	Confidential waste or shredding	Retain confirmation that vetting was carried out, the result and the recruitment decision taken

Schedule B: **Employee HR Records**
Best practice guidance from Information Commissioner's Office, Chartered Institute for Personnel Development and Buzzacott Accountants

	Information	**Storage**	**Retention Period**	**Destruction method**	**Reason and/or Notes**
B1	Employee HR folder (incl. disciplinary and working time records)	Locked cupboard/ electronic systems password protected	6 years from last date of employment	Confidential waste or shredding	Limitations Act 1980
B2	Training records	Transferred to HR file when employment ceases/ electronic systems password protected	6 years from last date of employment	Confidential waste or shredding	Limitations Act 1980
B3	Employee summary spread sheet	Encrypted file	Permanent	N/a	Incl. employee no, name, DOB, start & end date, reason for leaving, leaving salary, pension contribution %, date HR file to be destroyed
B4	Parental leave	HR file in locked cupboard/ electronic systems password protected	5 years from birth/adoption of the child or 18 years if the child receives disability allowance	Confidential waste or shredding	
B5	Statutory maternity pay records, calculations, certificates (Mat B1s) or other medical evidence	HR file in locked cupboard/ electronic systems password protected	3 years after the end of the tax year in which the maternity period ends	Confidential waste or shredding	Statutory Maternity Pay (General) Regulations 1986 as amended

B6	Salary/wage records (including expenses and any overtime or bonuses)	Central records in locked cupboard/ electronic systems password protected	6 years	Confidential waste or shredding	Taxes Management Act 1970
B7	Statutory Sick Pay records, calculations, certificates, self-certificates	HR file in locked cupboard/ electronic systems password protected	3 years after the end of the tax year to which they relate	Confidential waste or shredding	Statutory Sick Pay (General) Regulations 1982 as amended
B8	Actuarial valuation reports	HR file in locked cupboard/ electronic systems password protected	Permanent	n/a	
B9	Money purchase details	HR file in locked cupboard/ electronic systems password protected	6 years after transfer or value taken	Confidential waste or shredding	
B10	Redundancy detail, calculations of payments, refunds and any notification to the Secretary of State	HR file in locked cupboard/ electronic systems password protected	6 years from date of redundancy	Confidential waste or shredding	
B11	Signing in/out records	Cupboard	6 years from 1st of January each year	Confidential waste or shredding	
B12	Records relating to the health of staff, occupational health, health questionnaires, medical clearance, work adjustments	Separate section within HR file/ electronic systems password protected	12 years after commencement	Confidential waste or shredding	Common practice

B13	CEO and Senior Leadership Team records	HR file in locked cupboard/ electronic systems password protected	10 years	Confidential waste or shredding	MYT business need (for historical purposes)
B14	Safeguarding allegations against an MYT employee or volunteer	HR file and copy given to the individual employee/ electronic systems password protected	Until the employee reaches retirement age or for 10 years if that is longer	Confidential waste/shredding	Working Together 2013
B15	Performance information including probation reports, practice Observations, appraisals and 1:1s	HR file/ electronic systems password protected	6 years after leaving date	Confidential waste or shredding	

Schedule C: **Governance records**
Best practice guidance from Information Commissioner's Office, Charity Commission, Companies House and Chartered Institute for Personnel Development

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
C1	Companies House and Charity Commission appointment and termination records	Logged within the Companies House and Charities Commission secure portal	Permanent	N/a	MYT business need
C2	Personal information of Directors & Company Secretary required for Companies House registration	Logged within the Companies House and Charities Commission secure portal	48 hours until registration confirmed	Delete from Inbox, Sent box and Trash folders. Confidential waste/shredding	GDPR
C3	Trustee Board Minute	Stored digitally within a secure area	Permanent	n/a	Charities Act, Companies Act, MY Trust business need
C4	Trustee summary spreadsheet (Trustee name, start & end date of office)	Encrypted computer file	Permanent	n/a	MY Trust business need
C5	Organisation structure charts	digital files	Permanent	n/a	MY Trust business need
C6	Contracts with customers, suppliers or agents	Cupboard and digitally stored	6 years after expiry or termination of the contract	Confidential waste/shredding	Limitations Act 1980

Schedule D: **Health & Safety records**
Best practice guidance taken from Information Commissioner's Office, Health & Safety Executive and Chartered Institute for Personnel Development

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
D1	Assessments under health & safety regulations (annual and specific)	Locked cupboard or computer system	Permanent	N/a	Health & Safety Act 1974 as amended
D2	Records of consultations with employees	Locked cupboard and/or computer system	Permanent	N/a	Health & Safety Act 1974 as amended
D3	Accident, Incident and Near Miss completed records and reports (**employees, volunteers and Trustees**)	Locked cupboard and/or secure computer record	6 years	Confidential waste/shredding	RIDDOR 1995
D4	Accident, Incident and Near Miss completed records and reports (**children and young people**)	Locked cupboard and/or secure computer record	Date at which young person reaches age 21 (or 6 years whichever is the longer)	Confidential waste/shredding	RIDDOR 1995
D5	COSHH assessments and tests	Cupboard	5 years from date on which tests carried out	Confidential waste/shredding	COSHH Regulations 1999 and 2002
D6	Assessments and reports identifying presence of asbestos	Cupboard	5 years with review and decision before destruction	Confidential waste/shredding	Control of Asbestos at Work Regulations 2002

D7	Written plans to control asbestos	Cupboard	5 years with review and decision before destruction	Confidential waste/shredding	Control of Asbestos at Work Regulations 2002
D8	Fire Certificates	Cupboard	3 years	Confidential waste/shredding	Fire Precautions Act 1971
D9	Fire fighting equipment inspection reports	Cupboard	3 years from date of report	Confidential waste/shredding	MYT business need
D10	Fire evacuation reports	Cupboard	3 years	Confidential waste/shredding	Fire Precautions Act 1971

Schedule E: **Accounting records**

Best practice guidance taken from Information Commissioner's Office, Chartered Institute for Personnel Development and Buzzacott Accountants

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
E1	Annual Accounts and Trustee Report	Cupboard and digitally stored	Permanent	n/a	GDPR
E2	Accounting records (paper)	Cupboard	6 years from financial year end	Confidential waste/shredding	s221 of Companies Act 1985 and Charities Act
E3	Accounting records (electronic)	Computer system	Permanent		
E4	Petty Cash records (paper and electronic)	Cupboard	10 years	Confidential waste/shredding	Companies Act, Charities Act and HMRC
E5	Fixed Asset Register(paper/electronic)	Cupboard File on computer	Permanent	n/a	Companies Act, Charities Act, MYT business need
E6	Invoices for capital items	Cupboard and computer system	10 years	Confidential waste/shredding	Companies Act, Charities Act and HMRC

E7	Income tax and national insurance returns, income tax records (eg P45) and correspondence with HMRC	Cupboard and computer system	6 years plus current year	Confidential waste/shredding	In line with Income Tax (Employments) Regulations 1993 as amended
E8	Deeds of covenant/gift aid declarations	Secure cupboard and digital file	6 years after last payment; 12 years if payments outstanding or deed dispute	Confidential waste/shredding	GDPR
E9	Notice to employer of tax code	HR file/Payroll Folder and HR digital system	6 years plus current year		Taxes Management Act
E10	Certificate of pay and tax deducted (P60).	Employees online login (permanent)	3 years		Taxes Management Act
E11	Payroll and payroll control account.	Secure cupboard/computer system.	6 years plus current years		Companies Act, Charities Act and Taxes Management Act
E12	Expense accounts and records	Cupboard and electronic file	6 years plus current year	Confidential waste/ shredding for paper records	Taxes Management Act

Schedule F: **Buildings and plant records**

Best practice guidance from Information Commissioner's Office and Buzzacott Accountants

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
F1	Leases	Cupboard	15 years after expiry	Confidential waste/shredding	Limitations Act 1960
F2	Asbestos register and asbestos disposal certificate	Cupboard	Permanent	N/a	Control of Asbestos at work Regulations

F3	Records of major refurbishments, warranties, planning consents, design documents	Cupboard	13 years then review before destruction	Confidential waste/shredding	GDPR

Schedule G: **Insurances**

Best practice guidance from Information Commissioner's Office and Buzzacott Accountants

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
G1	Policies	Digital storage, HR system	3 years after lapse	Confidential waste/shredding	GDPR
G2	Claims correspondence	Cupboard	3 years after settlement	Confidential waste/shredding	GDPR
G3	Employer's Liability insurance certificate	Cupboard/digital/uploaded on HR system	40 years	Confidential waste/shredding	Employer's Liability (Compulsory Insurance) Regulations 1998

Schedule H: **Service delivery partnerships**

Best practice guidance from Information Commissioner's Office and Buzzacott Accountants

	Information	Storage	Retention Period	Destruction method	Notes
H1	Service contracts with customers (eg TrustCareers contracts with schools)	Cupboard and digital storage on shared access	6 years after expiry or ending of contract	Confidential waste/shredding	Limitations Act 1980
H2	Service contracts with suppliers (eg contracts with agencies or contracted staff)	Cupboard and or digital	6 years after expiry or ending of the contract	Confidential waste/shredding	Limitations Act 1980
H3	Service contracts with Commissioners and funders	Cupboard and/or digital	6 years after expiry or ending of the contract	Confidential waste/shredding	Limitations Act 1980
H4	Partnership Agreements and Service Agreements with partners	Cupboard and/or digital storage	6 years after expiry or ending of the contract	Confidential waste/shredding	Limitations Act 1980

Schedule I: **Safeguarding, child protection, children in need and CLA**

Best practice guidance from Information Commissioner's Office, NSPCC, Working Together to Safeguard Children 2013 and Guidance to Social Services 2000

	Information	Storage	Retention Period	Destruction method	Notes
I1	Child welfare concerns referred to social care or police	Salesforce	6 years and then reviewed	Archived and end of retention for three further years then deleted	
I2	Child welfare concerns NOT referred to social care or police	Salesforce	Young person's 19th birthday	Record archived until 25th birthday then destroyed	

I3	Young people's records in which the young person has received individual social care child protection case assessment, investigation, registration and management: • Investigated, conferenced & registered • Core assessment • Investigated but not conferenced & registered	Salesforce	35 years from case closure. Held within archived records once young person turns 25 years	Digital file deletion	Shared practice with local authorities
I4	Children in Need who have not been adopted or looked after and who have not been the subject of a child protection enquiry	Salesforce	10 years from closure of case, then archived to young person's 25th birthday	Digital file deletion	Shared practice with local authorities
I5	Assessment of a family's suitability in the care of children	Salesforce	25 years from DOB of youngest child. Archived five years after date of last contact	Digital file deletion	Shared practice with local authorities
I6	Safeguarding allegations against an MY Trust employee or volunteer	HR file and copy given to the individual employee	Until the employee reaches retirement age or for 10 years if that is longer	Confidential waste/shredding	Working Together 2018

I7	Concerns about people (paid and unpaid) who work with children and young people. A record of the behaviour, the action taken and outcome should be recorded.	HR files or separate secure file	6 years after employment ends or until person reaches retirement age (or 10 years if longer) if concerns a child may have been harmed, the adult may have committed a criminal offence against child or the adult behaviour indicates unsuitable to work with children	Confidential waste/shredding	Working Together 2018

Schedule J: **General service delivery – service users' records**

Best practice guidance from Information Commissioner's Office, Data Protection Act, CCIS Guidance, commissioned contracts

	Information	**Storage**	**Retention Period**	**Destruction method**	**Notes**
J1	Handwritten notes of discussion with a young person	Secure cupboard	1 week then typed up or scanned	Confidential waste/shredding	GDPR
J2	Electronic Documents	MS One Drive (Encrypted Device if on Residential)	1 week after end of Programme	Digital File Deletion	GDPR
J3	Photographs & Videos on Personal Devices	Personal Device (not in cloud)	Within 1 week of image being captured	Digital File Deletion	If signed BYOD acceptable use policy

J4	Photographs & Videos	MS One Drive or Encrypted External Hard Drive	1 full academic year after the image was taken	Digital File Deletion	GDPR
J5	Qualification Portfolios	Chatham Archive	7 Years	Confidential waste/shredding	Examination Board - NOCN
J6	Digital client record for young people accessing services	Relevant Database	1 full academic year after intervention or programme, or when contract ends	Data Anonymised	GDPR

Policy:	**Information Security Management Policy**
Approved by Chief Executive:	
Approved by Trustees:	
Policy Review (12 months or earlier depending on legislative changes):	