5.8 Record Retention and Deletion Policy

The Adventure Service Ltd.

Last Reviewed	**3rd May 2024**
Reviewed By (Name)	**Helen Harris-Ellis; Daniel Barrow**
Job Role	**Director**
Next Review Date	**Before May 2027**
V2.1 February 2021	Formatting review Examples now given of what constitutes a 'major incident' with regards trips and outings. Amendments to the retention of DBS copy certificates.

Contents

1.1 Introduction

This record retention and deletion policy contains recommended retention periods for the different record series created and maintained by The Adventure Service Ltd. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines, following best practice, employed by services throughout the United Kingdom. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 (DPA), Article 8, the Human Rights Act 1998, the Freedom of Information Act 2000 (FOI) and the Code of Practice on Records Management (under Section 46 of the FOI).

Managing records series using these retention guidelines will be deemed to be 'normal processing' under the terms of the legislation noted above. If those record series are to be kept for longer or shorter periods than the time scales held in this document, the reasons for any deviation must be recorded.

This policy will be reviewed at intervals of no more than three years, or exceptionally, if required by changes in Data Protection, Freedom of Interest or other legislation, where relevant.

1.2 Purpose

All services need to create and maintain accurate records for them to function and carry out the tasks of educating, developing and safeguarding clients. This policy, for managing records at The Adventure Service Ltd has been drawn up in conformity with legislation, regulations affecting businesses and best practice as promoted by the Information and Records Management Society of Great Britain.

This policy sets out guidelines for recording, managing, storing and the disposal of data, whether they are held on paper or electronically (including online), in order to assist staff, and The Adventure Service Ltd, to comply with the General Data Protection Regulation (2018) and the Freedom of Information Act (2000). It should be read and used in conjunction with the following service policies;

- Management Information Systems
- Data Protection Policy
- Privacy Notices
- DPIA Information Asset Register

The implementation of the General Data Protection (2018) did not fundamentally change the principles around the duration of records retention. However, it has introduced stricter rules about the use and storage of personal data, requiring more dynamic, efficient and secure storage systems. It is expected that;

- All information held by providers needs to be justifiable, by reference, to its purpose.
- Businesses must be transparent and accountable as to what data they hold.
- Businesses must understand and explain the reasons why they hold data.
- Businesses must be able to respond to Subject Access Requests.
- Businesses must be able to amend, delete or transfer data promptly upon any justified request.
- Businesses must be able to audit how personal data was collected and when and why.
- *Businesses must hold sensitive data securely, accessed only by those with reason to view it and possess a policy as to why it is needed.*

All members of staff, with access to records, are expected to;

- Manage their current record keeping systems using the Retention Policy.
- Only dispose of records in accordance with the requirements outlined in this policy, if authorised to do so.
- Ensure that any proposed divergence from the records retention schedule and disposal policies is authorised by the Directors.

This policy does not form part of any employee's contract of employment and is not intended to have a contractual effect. However, it does reflect The Adventure Service Ltd.'s current practice, the requirements of current legislation and best practice and guidance. It may be amended by The Adventure Service Ltd but any changes will be notified to employees within one month of the date on which the change is intended to take effect. The Adventure Service Ltd may also vary any parts of the procedure, including time limits, as appropriate.

1.3 Why hold a Retention Policy?

There are a number of benefits which arise from the use of a Retention Policy:

- Managing records against the Retention Policy is deemed to be 'normal processing' under the GDPR (2018) and the Freedom of Information Act (2000). Where members of staff are managing records using the Retention Policy, they will not be culpable of tampering or the unauthorised alteration of data, once a Freedom of Information request or Subject Access Request (SAR) has been made.
- Members of staff can be confident about destroying information at the appropriate time and in a secure fashion.
- Information which is subject to Freedom of Information and GDPR legislation will be available, when required.
- The school is not maintaining and holding information unnecessarily.

1.4 Examples of How Adventurer Records May Be Stored and the Information Shared.

The following examples illustrate a number of options by which Services may hold data – in some cases, where information is held on different platforms, a combination of these options may be employed ('hybrid files'). It is advised that the service, working with their Data Protection Officer, creates a summary of what information they hold and how;

Adventurer record (electronic) - 'a record is held on the service's electronic Management Information System (Hubspot and Microsoft Teams), from information provided by the Adventurer's parents/carers upon admission. Information includes; Adventurer name, address, emergency contact details and daily attendance.

Medical Records – 'information regarding the medical needs of an Adventurer is provided by parents/carers upon admission and updated, where necessary, following the annual review. Information provided includes any significant known reactions to medication, major allergies and notable medical conditions. This information is available to staff likely to administer medication or treatment. The information is shared externally or to external agencies only with parental/carer permission. This is information is held under the terms of the retention schedule, following the completion of the trip, or, for the duration of the Adventurer's time at The Adventure Service Ltd.

Financial Records – 'financial records are held electronically on Intuit Quickbooks

1.1.2 Emails, Texts and Instant Messaging

Emailing is a form of communication – it is not a means of storing information that may be kept securely elsewhere. Emails should not be kept, but rather transferred, if the information they hold falls into the categories listed within the Retention Schedule e.g. does it form part of an Adventurer record? Does it relate to an employee or a decision about an employee? If so, this information could be transferred to the Adventurers file, and the email deleted. Emails and attachments which hold data must not be kept as emails; they must be either be saved in an appropriate electronic management information system or printed off and filed as a hard copy document.

Services should consider implementing a rule whereby emails are automatically deleted after a period of time, once they have been filed, and make this known via their Data Protection Policy. Such a rule would limit the amount of information that might be available to a data subject under a Subject Access Request and helps reduce the amount of electronic storage required by The Adventure Service Ltd.

Similarly, texts, Instant Messages (e.g. WhatsApp, Facebook Messenger) or message boards and forums are not considered a permanent record of being ephemeral and temporary. If the content of the message or text is significant e.g. a staff member highlights concerns around an Adventurer's behaviour, then it should be copied and transferred into the appropriate filing system e.g. a safeguarding case file, either by saving it in a readable electronic format, or printing it off, or taking a screen shot.

Any information recorded within texts, Instant Messages, message boards or forums is subject to the same Data Protection and Freedom of Information legislation, regardless of format. Therefore, it is advisable to only use these methods of communication to transmit information which is not sensitive or directly related to a third party. Similarly, with regards emails, all electronic communications, whilst they are held by The Adventure Service Ltd, are disclosable under the same legislation and anything written or held, within an email, could potentially be made public under the terms of a Subject Access Request.

1.1.3 Social Media

Many providers will maintain some form of social media channel, such as Twitter or Facebook, with which to communicate with staff and parents. It should be noted though that social media is not just a means of communication, but can also act a repository for storing information and third party data. Information held in this format is subject to the Freedom of Information Act 2000 and the Data Protection Act 2018.

Social media outlets have different retention periods. Service's must be aware of how long these periods are, outline this within their Data Protection Policy and secure the appropriate consent to share personal data to enable the rights of the data subject. The Adventure Service Ltd needs to ensure that the primary users (i.e. those staff members who hold administrative permissions, to upload and remove information) are aware of these retention periods. Where these retention periods are longer than that set out as part of a standard policy or best practice e.g. removing Adventurers images from the service's website when that Adventurer has left, processes must be in place to remove any posts or photographs on a regular and routine basis.

Social media posts can remain online for a period long after the service has deleted them. They can be shared and redistributed many times, beyond the control of the individual who first posted them. In these instances, it is vital that the service is clear when obtaining the consent to share data, from Adventurers, parents, staff and volunteers, as to where information will be shared, for how long and outlining the risk of information being shared, or cached, beyond their control.

1.5 Access to Records

For the efficient running of The Adventure Service Ltd, all Instructional staff and relevant office staff will have access to The Adventure Service Ltd Management Information System (Hubspot and Microsoft Teams). Instructional staff may complete some the following functions e.g. enter names on the register or add other agency involvement, and may consult the Adventurer record

All permissions to access data are granted by the Directors and recorded in the member of staff's personnel file.

All Instructional and office staff will be given training and guidance on accessing and managing service records, to ensure compliance with the time scales laid out under the retention schedule. As a guiding principle the General Data Protection Regulation requires that personal data is only retained for as long as is necessary and for the specific lawful purpose(s) it was acquired; all information, held by the service must be kept in accordance with The Adventure Service Ltd.'s Data Protection Policy.

1.6 Data Protection Policy

Adventurers, parents and members of staff are informed, via The Adventure Service Ltd.'s Data Protection Policy (Data Protection Policy) that any information held on them, upon either admission or commencement of employment, is for The Adventure Service Ltd to carry out statutory functions, necessary for the efficient operation of the setting – data held will be reviewed regularly and will be stored, processed and shared (where appropriate and applicable) under the terms of the General Data Protection Regulation (2018).

1.6.1 Retention Periods

The following tables provide guidance on retention period for the different records held by The Adventure Service Ltd. Unless there is a specific statutory obligation to hold or destroy records the retention periods are established by The Adventure Service Ltd for guidance purposes.

1.6.2 Disposal of Data

As mentioned above, the fifth Data Protection principle, states that 'Personal data processed for any purpose, or purposes, shall not be kept longer than is necessary for that purpose, or purposes'. It is the responsibility of the Directors that records, which are no longer required for business use, are to be reviewed as soon as possible, so that the appropriate records can be destroyed or transferred, where necessary.

Not all data needs to be destroyed. The Adventure Service Ltd should determine whether records are to be selected, either for permanent preservation, or for destruction or to be transferred into a different format e.g. digitised, or to be retained further, by the setting, for research or litigation purposes. Any decision, which results in a change to the way data is held in the setting, must be documented as part of the records management policy. For example; financial records can be destroyed after six years, plus the year they were created in, and are often shredded or passed to a confidential waste provider for safe destruction.

When information is no longer required, it should be disposed of. For confidential, sensitive or personal information, to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. It is recommended that paper documents are destroyed with a cross shredder – where this is not possible, and, e.g. a ribbon shredder is employed, the waste should not be recycled but destroyed beyond recognition e.g. via an incinerator bin.

Skips and 'regular' waste disposal are not considered to be secure.

CD's/DVD's/discs should be cut into pieces. Hard copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal companies are employed, they should, wherever possible be supervised

and any destruction of data or removal of data, from the site, is logged and the destruction certified. Staff working for external provider should have been trained in the handling and destruction of confidential data.

Destruction of data will be planned with specific dates and all records will be identified as to the date of destruction. N.B. if a record is noted pending destruction or transfer, either to archives off site or to another setting, but has not yet been destroyed/transferred, and a request for records has been received, that record must still be made available to the requestor.

The Freedom of Information Act 2000 requires the service to maintain a list of all records that have been destroyed and who authorised their destruction. The appropriate members of staff (Data Lead) should record;

- File reference and/or unique identifier
- File title or brief description of contents
- Number of files
- Name of the authorising officer

1.8 Transfer of Records to other Media

Where lengthy retention periods have been allocated to records, member of staff may wish to consider converting paper records to other media (e.g. digital or virtual, 'cloud' based). The lifespan of the media, and the ability to migrate data, should always be considered.

1.9 Responsibility and Monitoring

The Directors and/or officer tasked with the role of Data Lead, hold primary and day to day responsibility, for implementing this policy. The Data Protection Officer, in conjunction with The Adventure Service Ltd, is responsible for monitoring its use and effectiveness and resolving any queries with regards the interpretation of the policy. The Data Protection Officer will consider the suitability and adequacy of this policy and will pass any amendments or alterations directly to the Director.

Internal control systems and procedures will be subject to regular audits, to provide assurance that they are effective in creating, maintaining and removing records.

1.11 Outline Retention Schedule

FILE DESCRIPTION	RETENTION PERIOD
1.11.1 Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the service has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	2 years after employment ceases
Immigration checks	2 years after the termination of employment
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel and training records	while employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations:	Two years from the date on which they were entered into

· Opt out forms · Records of compliance with WTR	Two years after the relevant period
Disciplinary and training records	6 years after employment ceases
Allegations of a child/adult protection nature against a member of staff including where the allegation is founded	until the person's normal retirement age or 10 years from the date of allegation, whichever is longer, then review. NB – allegations that are found to be malicious should be removed from personnel files, from the date they are proven to be unfounded.
1.11.2 Financial and Payroll Records	
Pension records	Current year + 6 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	Current year + 6 years
Payroll and wage records	Current year + 6 years
Maternity/Adoption/Paternity Leave records	Current year + 3 years
Statutory Sick Pay	Current year + 3 years
1.11.3 Agreements and Administration Paperwork	
Development Plans	Life of plan + 6 years
Professional Development Plans	Life of the plan + 6 years
Visitor management systems (including electronic systems, visitors books and signing in sheets)	Current year + 6 years

Newsletters and circulars to staff, parents and Adventurers	Current year + 1 year
1.11.4 Health and Safety Records	
Health and Safety Policy Statements	Life of the policy + 3 years
Health and Safety Risk Assessments	Life of the assessment + 3 years
Any reportable accident, death or injury in connection with work	Date of the incident + 3 years
Accident reporting	Adults – Retain for 7 years from the date of the accident Children – Retain for 25 years from the child's date of birth
Fire precaution log books	Current year + 3 years

1.12 Full Retention Schedule

Data Retention Schedule 2022					
Document type	**Purpose**	**Retention Period**	**Format**	**Location**	**Action**
Adventurer (Managers)					
Medication Administration		4 years after the date of Administration	Digital files	SharePoint/archive/medication Administration	Secure Disposal
Annual Reviews	To ensure that the service is meeting the needs of the Adventurer	6 years after date of review	Digital	Teams	Secure Disposal
Support plans	To enable the correct support to be given to Adventurers	3 years after last date of contact	Digital	Teams: Hubspot	Secure Disposal
Contact Details	To enable contact for Marketing and support purposes	3 years after last date of contact	Digital	Hubspot	Secure Disposal
Registers	To confirm attendance at the service	6 years	Digital	Microsoft Forms	Secure Disposal
All correspondence relating to a specific Adventurer should be filed in the appropriate filing system	To assist in providing a safe and stimulating service to Adventurers	Current year + 1-year Review to see whether correspondence still needed operationally then assign a new review date or destroy	Emails, Paper and Digital	Hubspot	Secure Disposal
Incident of aggression	To monitor behaviour and ensure safety of Adventurers	Date of the incident + 4 years	Digital	Microsoft Forms After one year moved to SharePoint/Archive/Accident-Incident	Secure Disposal
Safeguarding (Directors)					
Records relating to safeguarding	To ensure that we are meeting the safety	10 years from date of last contact	Paper and Digital files	Safeguarding File on Microsoft Teams Lockable cabinet in the admin office	Secure Disposal

	requirements for Adventurers				
Finances (Business Functions Manager)					
Financial records	To enable financial auditing to be undertaken.	Current year plus 6 years	Digital and paper files	Quickbooks Admin office	Secure Disposal
Final accounts	To enable financial auditing to be undertaken.	Permanent	Paper	Small locked office	Never
Purchase Order Forms	For proof of purchase and despatch of orders.	1 year from date on form	Paper	Teams	Shredding
Insurance documents	For proof of cover	7 years from date of policy	Digital and paper	Sharepoint/Archive/businessinsurance: Admin Office	Secure Disposal
Human Relations (Helen and Business Administrator)					
Staff contact details including name, address, DOB, emergency contact	To ensure the service can contact next of kin in emergencies.	3 years from termination of contract Emergency contact delete on termination of contract	Digital files	On teams: Hubspot	Secure Disposal
Staff questionnaires	To ensure that we are supporting the team	Date of questionnaires plus 6 years	Digital and paper	Microsoft Forms	Secure Disposal
Records relating to the monitoring of employee absence	To monitor absence and wellbeing of staff	Current year + 1 year	Digital	Teams/Sharepoint: Timetastic	Secure Disposal
Records relating to employment tribunal	To provide a fair and equitable process	Current year + 6 years	Digital	Teams/Sharepoint	Secure Disposal
First warning	To provide a fair and equitable process	Date of warning + 6 months [This period could be extended if required to be used for evidence to show that the employee was made aware of	Digital	Teams/Sharepoint	Secure Disposal

		the seriousness of previous behaviour]			
Second warning	To provide a fair and equitable process	Date of warning + 12 months [This period could be extended if required to be used for evidence to show that the employee was made aware of the seriousness of previous behaviour]	Digital	Teams/Sharepoint	Secure Disposal
Final warning	To provide a fair and equitable process	Date of warning + 18 months [This period could be extended if required to be used for evidence to show that the employee was made aware of the seriousness of previous behaviour]	Digital	Teams/Sharepoint	Secure Disposal
Personal Files records relating to an individual's employment history: Employment agreements Exit letters Training cost agreements etc	To meet legal obligations	Termination of employment + 6 years	Digital	Teams/Sharepoint	Secure Disposal
Progress meeting notes	To ensure that staff opinions are heard to record case discussions.	Termination of employment + 3 years	Digital	Teams/Sharepoint	Secure Disposal

Medical certificates presented in line with sickness reporting procedures	To monitor Staff Sickness and reveal potential patterns	Tax year to which they relate + 3 years	Digital	Teams/Sharepoint	Secure Disposal
Pay Timesheets/pay details Pay-rise letters P60s Payslips	To ensure that staff have been paid correctly	Current year + 10 years	Digital	Quickbooks Teams-Finance	Secure Disposal
Records relating to employee induction	To provide a fair and equitable induction process	Date induction ends + 6 months then review	Digital	Teams/Sharepoint	Secure Disposal
The selection of an individual for an established position	To prove a fair and equitable process occurred	Recruitment finalised + 1 year	Digital	Teams/Development Team/Recruitment month and year of recruitment	Secure Disposal
Recruitment and Selection – records relating to the process concerning unsuccessful candidates	To prove a fair and equitable process occurred	Date of interview + 6 months	Digital	Teams/Development Team/Recruitment month and year of recruitment	Secure Disposal
Copy documentation taken as part of right to work evidence	To meet statutory requirements	Date of termination of employment + 2 years	Digital	Teams/Sharepoint	Secure Disposal
DBS Information	To meet statutory requirements	Date of termination of employment + 3years	Digital	Checked on single central record Teams – safeguarding- single central record	Secure disposal
Identity documents	No right to keep this information				Secure Disposal
Training (Helen)					
Staff training records – general Positional contract and development pathways	To evidence training provided	Current year + 3 years	Digital	Teams/Sharepoint	Secure Disposal

Spreadsheets monitoring training provision	To evidence training provided	Operational use	Digital	Teams/Development Team/Staff training	Secure Disposal
Training (proof of completion such as certificates, awards, exam results)	To evidence training provided	Last action + 7 years	Digital	Teams/Sharepoint	Secure Disposal
Learning and Development: Course information and attendance lists	To check who has attended specific training	Current year + 3 years	Digital	Teams/Development Team/Staff training	Secure Disposal
Health and Safety (Terry)					
Accident/incident Reporting including COSHH	To meet health and safety regulations	Date of the accident + 4 years where the injured person is an adult at the time of the accident; date of birth + 22 years where the injured person is a minor at the time of the accident	Paper and Digital	Teams/The Adventure Service/Paperwork/Accident-Incident. After one year moved to SharePoint/Archive/Accident-Incident	Secure Disposal
Records relating to the Reporting of Injuries Diseases Dangerous Occurrences Regulations (RIDDOR) process	To meet health and safety regulations	the date of notification + 3 years	Paper and Digital	Teams/The Adventure Service/Paperwork/Accident-Incident. After one year moved to SharePoint/Archive/Accident-Incident	Secure Disposal
Records relating to health and safety training	To meet health and safety regulations	Date of training + 7 years	Digital	Teams/Sharepoint	Secure Disposal
COSHH – risk assessments etc.	Control of hazardous substances	5 years	Digital	Teams/Sharepoint	Secure Disposal
Correspondence (all staff responsible for own emails and files) (Post book Amy)					

Correspondence - Examples may include e-mails and correspondence which relates specifically to an individual's work.	To assist in providing a safe and stimulating service to Adventurers	Emails 6 months then moved to a secure file if needed in the future Current year + 1-year Review to see whether correspondence still needed operationally then assign a new review date or destroy	Emails, Paper and Digital	Personal files and Outlook	Secure Disposal
Post books recording incoming and outgoing post	To record outgoing and incoming postal transactions	Current year + 2 years after last entry.	Paper	Admin office, admin desk	Secure Disposal - shredding
Marketing					
Records relating to the development, implementation and monitoring of each marketing plan	Ensure correct delivery of newsletter and to ensure that all the merchandise sold is recorded for auditing purposes	Current year + 3 years then review	Digital	Team/Marketing Mail Chimp	Secure Disposal
Photographs of Adventurers and Employees	To promote The Adventure Service through marketing	18 months unless permission is removed by the individual Adventurer	Digital	Google Photos Facebook Website	Secure Disposal
Videos of Adventurers and Employees	To promote The Adventure Service through marketing	5 years unless permission is removed by the individual Adventurer	Digital	Youtube Website	Secure Disposal
Website and flyers	To promote The Adventure Service through marketing	Indefinite if the Adventurer attends the service and we have permission	Digital and paper	Wix Teams- marketing- flyers	Secure disposal

		1 year after the Adventurer/staff member has left			
Social media	To promote The Adventure Service through marketing	Delete after one year	Digital	Facebook Instagram Linkedin	Secure dispsal
Meetings (Daniel)					
Team Meeting/Management Team meeting minutes	To keep a record of issues discussed	Date of meeting + 1 year then review	Digital	Meeting minutes on Microsoft Teams	Secure Disposal
Service Level Agreements (Helen)					
Service level agreements with partner organisations	To enable partner agencies to know what to expect from our service and what is agreed	Life of agreement + 6 years	Paper and Digital	Current agreements stored on teams/Education/Service Level Agreements. Archived after one year stored in SharePoint/Archive/Service Level Agreements	Secure Disposal
Parental Consents (Managers)					
Trailblazer	To ensure that parents are in agreement with the service being provided to the child	3 years from the 18th birthday	Paper and Digital	Teams/Sharepoint	Secure Disposal
Day Service	To ensure that parents are in agreement with the service being provided to the child	3 years from the 18th birthday	Paper and Digital	Teams/Sharepoint	Secure Disposal
Short Breaks	To ensure that parents are in agreement with the service being provided to the child	3 years from the 18th birthday	Paper and Digital	Teams/Sharepoint	Secure Disposal

Appendix A- Safe Retention of Records Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with Data Protection legislation. Taking measures to protect your records can ensure that:

• Your service can demonstrate compliance with the law and avoid data loss incidents;

• In the event of a major incident, your service should be able to stay open and will at least have access to its key administrative and Adventurer records.

An Information Security Policy should incorporate a Business Continuity Plan and should deal with records held in all media across all school systems:

• Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images)

• Hard copy (including but not limited to paper files, plans)

A1 Digital Information

In order to mitigate against the loss of electronic information a service needs to:

a. Operate an effective back-up system

You should undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Where possible these backups should be stored in a different building to the servers and if possible off the main service site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. Options for the management of back-up facilities include:

• Use of an off-site, central back up service (usually operated by the local authority or other provider). This involves a back-up being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the service.

• Storage in a data safe in another part of the service premises

The back-up may be stored in a fireproof safe which is located in another part of the premises. These premises must also be physically secure and any hard copy supporting data regarding the location of records should also be stored in the safe.

Where services make use of cloud storage instead of, or alongside, physical onsite servers, they should ensure that the location of the cloud storage and the security offered are appropriate for the information and records stored.

b. Control the way data is stored within the service

Personal information should not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c. Manage the location of server equipment

Ensure that the server environment is managed to prevent access by unauthorised people.

d. Ensure that business continuity plans are tested

Test restore processes on a regular basis to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it.

A2 Hard Copy Information and Records

Records which are not stored on the service's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access. Wherever possible, and where appropriate, if information can be stored electronically rather than hard copy, then store it electronically.

a. Fire and flood

The cost of restoring records damaged by water can be high but a large percentage may be saved; a fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water. Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard should be raised at least 2 inches from the ground. Physical records should not be stored on the floor.

b. Unauthorised access, theft or loss

Staff should be encouraged not to take personal data on staff or Adventurers out of the service unless there is no other alternative. Records held within the service should be in lockable cabinets. Consider restricting access to offices in which personal information is being worked on or stored. All archive or records storage areas should be lockable and have restricted access.

Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.

c. Clear Desk Policy

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood damage.

A clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

A3 Risk Analysis

Individual services should undertake a business risk analysis to identify which records are vital to service management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.

The development of an information asset/risk register can assist with this process.

A4 Responding to Incidents

In the event of an incident involving the loss of information or records the service should be ready to pull together an incident response team to manage the situation. Service's should have a process, which must be used by all members of staff, if there is a major data loss or information security breach. This will involve appointing a Data Protection Officer to liaise with the Information Commissioner's Office if an information security breach needs to be reported. Please be aware – a loss of data e.g. accidental destruction of records, is a data breach just as if those records had been lost, stolen or wrongfully shared.

A5 Maintaining an Archive

The Adventure Service Ltd generates a large amount of data that is not necessarily personal or sensitive, yet is worthy of retention as part of the setting's historical legacy; records, photographs, and fliers. These, and other items, document not only the service's past, but also reflect its place within the greater community. Sometimes The

Adventure Service Ltd may be asked what historical records are still maintained within the setting. Often these requests come from former Adventurers, when they need to provide proof of their attendance. Other requests come from family historians carrying out research on their family tree and about their ancestors.

A service archive is different from an official service records system – all services will have an established record-keeping system for official records and a Management Information System, which includes record-keeping guidelines. An archive preserves data, beyond the retention period, where there is a legitimate interest in holding that information e.g. to commemorate a significant event in the life of the service. It can take on many characteristics and serve many purposes--but it neither compliments nor replaces the official record-keeping systems. However, records held in an archive must be accessed the same way, as current service records, and it would be necessary for the service to prove the identity of anyone requesting historical information, in the same way they would a Subject Access Request. To comply with the General Data Protection Regulation, the services should consider the following, if a request has been made to consult someone else's personal information in school archive that is not in the public domain.

- Entries for an individual who is (or would be) more than one hundred years old can be viewed without restriction.
- If the individual is less than one hundred years old you would need to provide proof that that person is now deceased, and to supply a death certificate for them.
- If the requester wishes to access information still held under the terms of the retention schedule, they would need to make a Subject Access Request.

When creating an archive, a service should be aware that it must serve the purpose of repository for the collection and preservation of historically valuable documents, relating to the history of the service or the community, which otherwise would be lost.

