The Yehudi Menuhin School

Data Protection and Retention Policy

Revision History

Revision	Paragraph Number	Revision
Autumn 2022	Whole document	New policy extracted from staff handbook Bursar & COO now named as Data Protection Lead

Click here to enter text.

Summer 2024	Whole document	ISBA Template used with updated timings, adapted to YMS context

Abbreviations, Acronyms and Definitions

Abbreviation / Acronym	**Definition**
ICO	Information Commissioner's Office
GDPR	General Data Protection Regulation (2018)

Click here to enter text.

Part A: Data Protection

Background

1. Data protection is an important legal compliance issue for The Yehudi Menuhin
2. School (the "School"). During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as data "controller", is liable for the actions of its staff and its trustees/governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.
3. UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.
4. Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office ("ICO") is responsible for enforcing data protection law in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Definitions

5. Key data protection terms used in this data protection policy are:
6. Data Controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its trustees/governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
7. Data Processor – an organisation that processes personal data on behalf of a controller, for example an IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
8. Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
9. Personal information (or 'personal data'): any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not

simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

10. Processing – virtually anything done with personal data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

11. Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

Application of this policy

12. This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

13. Those who handle personal data as employees or governors/trustees of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

14. In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

15. Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

16. If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

17. This Policy will inevitably have some overlap or interaction with other policies concerning how staff handle data, notably:

- Policy for the Acceptable Use of IT
- Safeguarding and Child Protection Policy
- Privacy Notices
- Staff Code of Conduct

Person responsible for Data Protection at the School

18. The School has appointed The Bursar as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

The Principles

19. The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

- Processed **lawfully, fairly** and in a **transparent** manner;
- Collected for **specific and explicit purposes** and only for the purposes it was collected for;
- **Relevant** and **limited** to what is necessary for the purposes it is processed;
- **Accurate** and kept **up to date**;
- **Kept for no longer than is necessary** for the purposes for which it is processed; and
- Processed in a manner that ensures **appropriate security** of the personal data.

20. The UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

21. keeping records of our data processing activities, including by way of logs and policies;

22. documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and

23. generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notices were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Lawful grounds for data processing

24. Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

25. One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its privacy notices, as the UK GDPR requires.

26. Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

Headline responsibilities of all staff

Record-keeping

27. It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Click here to enter text.

28. Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

Data handling

29. All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding and Child Protection Policy
- Acceptable Use if IT Policy for Staff
- Digital Media Policies
- CCTV Policy
- Whistleblowing Policy

30. Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

31. One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

32. In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify The Bursar. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

33. As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

34. More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 5 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

35. We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to The Bursar, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

36. As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to The Bursar in the first instance, and at as early a stage as possible.

Rights of Individuals

37. In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell The Bursar as soon as possible.

38. Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

- None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:
- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

  In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell The Bursar as soon as possible.

Data Security: online and digital

39. The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
40. Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data should as a minimum be password protected, with internal access restricted to those who need this information in order to perform their job role. The School has carefully selected the systems it uses to store digital records to ensure that they are held securely and employs two-factor authentication processes. The School also engages a specialist IT contractor to support it who ensures that the school IT system is secure.
41. No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
42. No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
43. School staff are permitted to access digital records whilst offsite however this must be done via the use of a School encrypted device or via the secure VPN link. School staff are not permitted to use their own devices to access digital records unless it is via the secure VPN link.
44. Use of personal email accounts or unencrypted personal devices by governors or staff for official School business is not permitted.

45. Any member of staff must be vigilant to the security of any network accessed away from the School premises. Open or unencrypted networks must not be used for School business, including data processing.

46. Files should not be downloaded and stored on personal devices including temporary download files on mobile phones.

47. Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments. They may also contain particular information: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) in a subject access request. Emails therefore can be particularly important. Staff are encouraged to consider an appropriate method of electronic filing such that relevant records can be more easily retrieved and/or deleted if required.

48. All digital records must only be stored on the School's secure server and should never be stored on hard drives of devices, USB sticks, portable hard drives etc.

Processing of Financial / Credit Card Data

49. The School complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

Part B: Storage and Retention of Records and Documents

1. The School has considered a variety of information when considering the retention periods stipulated in Appendix A of this policy and has had regard to all government regulation and advice.

The legal framework around data and document retention in the UK

2. The Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR), the retained UK version of GDPR following Brexit, are not prescriptive about the

length organisations are able to retain documents or data – although sometimes specific document retention periods are set out in other sources of law or guidance.

3. The rule under data protection law is based on principle: that personal data must not held for longer than is necessary for the particular lawful purpose for which it was collected. Nor should 'data controllers' keep more personal data than is necessary for that purpose.

4. In this way, UK GDPR requires schools to set policies reflecting these key data protection principles: but most actual retention periods are matters of judgment.

IICSA update (November 2022) and implications for document retention

5. The final report from IICSA recommended that any data relating to child sexual abuse (CSA) allegations should be kept for 75 years, but subject to regular review.

6. Schools should also be aware that the longer they hold large amounts of personal data, the more onerous their exposure to subject access or erasure requests and the risk of data security breaches. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not) – or details as to physical or mental health – should be kept securely, shared with or accessible to proper persons on a need-to-know basis.

Purpose of these guidelines

7. The School will generally seek to balance the benefits of keeping detailed and complete records – for the purposes of good practice, archives or general reference – with practical considerations of storage, space and accessibility. The following legal considerations apply in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including e.g. KCSIE;
- disclosure and evidence requirements for potential future litigation;
- contractual and insurance obligations;
- the laws of confidentiality and privacy; and (last but by no means least relevant)
- GDPR and the DPA, which enshrines it in UK law.

8. These will inform not only minimum and maximum retention periods but also what to keep and who should be able to access it.

Meaning of "Record"

9. In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material, but not all, will contain personal data of individuals as defined in GDPR.

10. The format of the record is less important for retention purposes than its contents, and the reason for keeping it (although format is of course an important consideration in terms of how best to preserve documents securely).

    Digital records

11. The process of digitisation of existing records is generally to be encouraged, however, digital records can be lost or misappropriated in huge quantities very quickly.

12. Access to sensitive data – or any large quantity of data – should as a minimum be password-protected (ideally with two-factor authentication), with internal access on a need-to-know basis.

    Email accounts and internal messaging systems

13. Emails and other internal messages – whether they are retained electronically or printed out as part of a paper file – are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments. As such they will potentially fall within the scope of a subject access request made against the school.

14. They may also contain particularly important information: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) in a subject access request.

15. Great importance of care and professionalism must be demonstrated in how such records are created by casual email (or other forms of instant messaging such as Teams, which are also records for these purposes). This will become particularly apparent when a subject access request is made by a colleague, pupil or parent and the data recorded may need to be provided.

16. It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes – or its deletion. Metadata may be necessary to examine under a legal claim or a data audit.

    Records on personal devices including SMS / WhatsApp

17. Whether text / WhatsApp messages, and any other files or notes held by a staff member or governor on their personal device (including tablet or smartphone) counts as a school "record" will depend on the circumstances.

18. As a general rule, an employee has an expectation of privacy in their own messaging for personal use, and is not subject to UK GDPR for solely domestic or 'household' uses of data.

19. However, where personal devices are used by employees or governors / trustees for official school use – for example to discuss a pupil issue, parental complaint or disciplinary matter – it may be deemed an official record of the School. This means it may be disclosable in litigation or under a subject access request, if the School has reasonable grounds to believe relevant evidence or personal data might be found on the device, including by SMS, WhatsApp or personal email. In that sense, any staff or governor WhatsApp group must be used with the same professional formality as email.

Secure Disposal of records

20. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot be either read or reconstructed.

21. For hard copy documents, skips and putting something into the regular rubbish (i.e. in waste bins around school or in offices) will not be considered secure. Paper records or images should be shredded using a shredder

22. Devices for digital storage and recordings (e.g. external hard drives, USB stick storage etc.) should be dismantled and broken into pieces.

23. For digital devices, a number of individual steps are advisable prior to disposal; wiping the hard drive and/or activating drive encryption; uninstalling and/or deauthorising applications or accounts that could enable a use to access secure school systems (including wiping browsing history and cookies); and or physically destroying the device. The School disposes of its digital devices using the services of its IT Contractor.

24. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the School to process and dispose of the information.

25. Further information and support is available to staff from the Bursar on request.

Appendix A – Table of Retention Periods

Type of Record/Document	Suggested Retention Period
EMAILS ON SERVER	
Pupil email account	Delete upon leaving school, or within one year.
Staff emails	Routine deletion of historic emails after 2-3 years, and delete account within 1 year of leaving school.
SCHOOL-SPECIFIC RECORDS	
Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then archive.
Minutes of Governors' meetings	6 years from date of meeting minimum
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	***NB these records will contain personal data***
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or up to 7 years from the pupil leaving). If unsuccessful: up to 1 year.
Student immigration records	Duration of student sponsorship plus min. 1 year
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: • Pupil reports and performance records • Pupil medical records (*not accidents*)	ALL: 25 years from date of birth (*subject where relevant to any material that may be relevant to potential historic claims: see below*).
Special educational needs records	Date of birth plus up to 35 years (*risk assessed*)
SAFEGUARDING	
Policies, procedures and insurance	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be

Child Protection files and specific records of child sexual abuse Video recordings of meetings	reviewed from time to time if resources allow and a suitably qualified person is available. If a referral has been made / social care have been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years. Where any one-on-one meetings of classes, counselling, or application interviews are recorded (e.g. for safeguarding purposes), a shorter-term retention policy is acceptable based on the DSL's view of how quickly a concern will likely be raised: e.g. 3-6 months or immediately upon DSL review.
CORPORATE RECORDS Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
Shareholder resolutions	Minimum – 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex members/shareholders)
Annual reports	Minimum – 6 years
ACCOUNTING RECORDS Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 6 years for UK charities from the end of the financial year in which the transaction took place
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.

• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
<u>EMPLOYEE / PERSONNEL RECORDS</u> Single Central Record of employees Contracts of employment Employee appraisals or reviews Staff personnel file	***NB these records will contain personal data*** Keep a permanent record that mandatory checks have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above) 7 years from effective date of end of contract Duration of employment plus minimum of 7 years As above, but <u>do not delete any information which may be relevant to historic safeguarding claims</u>
Payroll, salary, maternity pay records	Minimum – 6 years
Pension or other benefit schedule records	Potentially permanent (ie lifetimes of those involved), depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year (as CVs will rapidly be out of date)
Staff immigration records (Right to work, etc.) Tier 2 migrant worker sponsor records	Minimum – 2 years from end of employment Minimum – 1 year from end of employment
Health records relating to employees Records of low-level concerns about adults	7 years from end of employment At least until end of employment (as recommended by KCSIE), then subject to review for relevance: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes / claims.
<u>INSURANCE RECORDS</u> Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)
<u>ENVIRONMENTAL, HEALTH & DATA</u> Maintenance logs Accidents to children	10 years from date of last entry 25 years from birth (longer for safeguarding)

Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances Covid-19 risk assessments, consents etc. (for now: this to be subject to further review)	Minimum – 7 years from end of date of use Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results
Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.
MENUHIN HALL RECORDS Box office bookings, customer details	For as long as there is a 'legitimate interest;' the customer database will be reviewed every two years.
Private Hire contracts	Minimum 7 years from completion of contractual obligations or term of agreement, whichever is later
Recording agreements	Minimum 7 years from completion of contractual obligations or term of agreement, whichever is later
OTHER Staff /Visitor Signing In/Out logs	6 years

Click here to enter text.