DIXONS ACADEMIES TRUST

Records Retention and Data Management Policy

Responsibility for review: chief executive, Dixons Academies Trust
date of last review: November 2024

Policy document provenance

Approver:	School and college trust leaders
Date of approval:	April 2024
Version:	1.0
Policy owner:	Accounting officer
Date of next review:	September 2026
Summary of changes since last review:	• This is a new policy and incorporates the data classification, handling and disposal policy, data governance and records management policy • The policy includes recommendation 17: access to records from the Inquiry into Child Sexual Abuse (IICSA) which was published in October 2022
Related policies and documents:	• Data protection policy • DAT Freedom of information guidance • DAT Subject access request guidance

Unless there are legislative or regulatory changes in the interim, the policy will be reviewed as by the review cycle. Should no substantive change be required at this point, the policy will move to the next review cycle.

Contents

1.0 Policy statement

1.1 Section 46 of the Freedom of Information Act 2000 requires trusts, as public authorities, to follow a code of practice on managing their records. This policy highlights the organisational approach to data and information management to encompass the full life cycle of data from acquisition, to use, to disposal.

1.2 Everyone has a responsibility to look after our trust's data and abide by our data policies and all applicable laws including the UK general data protection framework (UK GDPR). Mismanagement of data by students, staff or others may lead to fines, reputational damage and can have other process and financial implications.

1.3 The retention period for each type of record is shown in Appendix 1 of this policy document. Data protection legislation makes it unlawful to keep the information when it is no longer needed for the purpose for which it is held. By having a policy which adheres to recognised retention periods and to have a system of categorising data will aim to protect information from accidental or deliberate compromise and, should data be compromised our trust has ensured that only the minimum amount of data has been lost. This will ensure that our trust meets our legal, ethical and statutory obligations.

1.4 This policy also includes the categorisation of information in relation to its sensitivity and confidentiality and to define rules for the handling of each category to ensure an appropriate level of security of that information.

2.0 Legal framework

2.1 This policy has due regard to legislation, including, but not limited to, the following:

- The UK General Data Protection Regulation
- The Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

2.2 This policy also has due regard to the following guidance:

- Information Records Management Society (2016) Information management toolkit for schools
- DfE (2018) Data protection: A toolkit for schools
- The code of practice on the management of records issued under section 46 of the Freedom of Information Act 2000

3.0 Scope of the policy

3.1 The objective of the policy is to prevent and limit the impact of information security problems that might damage our trust's operation, reputation or business.

3.2 This policy applies to all records created, received or maintained by all staff within our trust and our academies in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by our trust and which are thereafter retained (for a set period) to provide evidence of its transactions and activities. These records may be created, received or maintained in hard copy or electronic format, which include but are not limited to paper documents, scanned documents, emails which document business activities and decisions, audio and video recordings, text messages, spreadsheets, Word documents, presentations etc.

3.3 Occasionally, there may be circumstances which mean that a record should be kept for longer (for example where there is a risk of litigation or a request from an outside body such as the Independent Inquiry into Child Sexual Abuse ((IICSA).

4.0 Responsibilities

4.1 The board of trustees has a statutory responsibility to maintain our trust's records and record keeping systems in accordance with the regulatory environment specific to the sector. The audit and risk committee will approve the policy every two years unless legislation changes and a revised policy is required before the two-year review date.

4.2 The head of governance is responsible for the day-to-day operational management and will give guidance on good records management practice and promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely manner. The head of governance will also monitor compliance with this policy by surveying, at least annually, to check if records are stored securely and can be accessed appropriately.

4.3 The academy will manage the records disposal process in line with the retention schedule. This will help to ensure that it can meet freedom of information requests and respond to requests to access personal data under data protection legislation (subject access requests).

4.4 Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

- manage their department or academy's records consistently in accordance with this policy and procedure
- hold information securely
- only share personal information appropriately and do not disclose it to any unauthorised party
- dispose of records securely in accordance with the retention schedule.

5.0 Independent Inquiry into Child Sexual Abuse (IICSA)

5.1 The IICSA report was presented to Parliament in October 2022 and our trust must ensure that records are kept in accordance with recommendation 17 of the report:

The retention period for records known to relate to allegations or cases of child sexual abuse should be 75 years with appropriate review periods.

5.2 The range of documentation which might need to be kept is wide. It will include any information linked to alleged or established child abuse, whether by staff, volunteers or students, with no limitation date. For example, a list of students who attended an overnight academy trip or admissions registers which show which students were on roll within our trust at a given time. As such, documents should be kept for longer than the retention periods listed in the policy if they concern information which might be relevant to an inquiry.

6.0 Management of student records

6.1 Student records are specific documents that are used throughout a student's time in the education system – they are passed to each school that a student attends and include all the personal information relating to them. All information must be easy to find, accurately and objectively recorded and expressed in a professional manner as students and parents have a right to access their educational record via a data subject access request. Please note that a request for an educational record under the Education (Pupil Information) (England) Regulations 2005 states that the student record must be supplied to parents within 15 days of a request. However, this only relates to maintained schools and not academies.

7.0 Records not forming part of the student record

7.1 The following record types should be stored separately to the main student record as they are usually subject to shorter retention periods and they should not be forwarded to the student's next school:

- attendance registers and information
- absence notes and correspondence
- accident forms (if it is a major incident, a copy can be placed on the student record)
- medicine consent and administering records
- copies of birth certificates, passports etc
- generic correspondence with parents about minor issues (eg 'Dear parent')
- student's work, drawings etc
- previous data collection forms which have been superseded
- photography consents

8.0 Transferring student records

8.1 Academies must ensure swift transfer of information to the new school to ensure appropriate decisions can be made regarding a student, using relevant and accurate information.

8.2 The following documents should be transferred to the next school within 15 working days of receipt of confirmation that a student is registered at another school:

- common transfer file (CTF) from the school information management system
- any elements of the student record, held in any format, not transferred as part of the CTF
- SEN or other support service information, including behaviour, as only limited information may be included in the CTF
- child protection information: this must be sent as soon as possible by the designated safeguarding lead or a member of their team to their equivalent at the new school

8.3 Academies must make sure the information is kept secure and traceable during transfer:

- records can be delivered or collected in person, with signed confirmation for tracking purposes
- student records should not be sent by post. If the use of post is absolutely necessary, they should be sent by 'special delivery guarantees' or via a reputable and secure courier to a pre-informed named contact, along with a list of the enclosed files. The new school should sign a copy of the list to confirm receipt of the files and securely return this to the previous school
- if held electronically, records may be sent to a named contact via secure encrypted e-mail or other secure transfer method

8.4 If the student is transferring to an independent school or a post 16 establishment, the existing school should transfer copies of relevant information only and retain the original full record as the last known school.

8.5 The last known or final school is responsible for retaining the student record. The school is the final or last known school, if it is:

- a secondary phase and the student left at 16 years old or for post-16 or independent education
- a school at any point and the student left for elective home education, they are missing from education or have left the UK

9.0 Retention schedule

9.1 The retention schedule, in Appendix 1, is divided into 7 sections:

1. Management and governance of the trust
2. Management of an academy
3. Student management
4. Human resources
5. Health and safety
6. Financial management
7. Property management

10.0 Data classification, handling and storage

10.1 All information held by or on behalf of our trust shall be categorised according to the information classification in Appendix 2.

10.2 Information shall be handled in accordance with the information handling rules and where the information falls within more than one category, the higher level of protection shall apply in each case.

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
1	**Management and governance of our trust**				
1.1	Instruments of government, Articles of Association and memorandum of understanding		For the life of the trust	Consult local archives before disposal	No
1.2	Trusts and endowments		For the life of the trust	Consult local archives before disposal	No
1.3	Annual report, accounts and financial statements	Academy trust handbook and HM Treasury	6 years	Secure disposal	No
1.4	Internal committee meeting minutes		6 years	Secure disposal	Potential
1.5	Minutes of trustees' meetings	Section 248 of the Companies Act 2006	Date of report + 10 years	Secure disposal	Potential
1.6	Agenda and papers for meetings	Section 248 of the Companies Act 2006	Date of report + 10 years	Secure disposal	Potential
1.7	Reports made to trustee meetings which are referred to in the minutes	Section 248 of the Companies Act 2006	Date of report + 10 years	Secure disposal	Potential
1.8	Register of attendance at trustee meetings		Date of last meeting plus 6 years	Secure disposal	Yes
1.9	Annual reports required by the DfE		Date of report + 10 years	Secure disposal	Yes
1.10	Minutes of AGM	Section 248 of the Companies Act 2006	Date of report + 10 years	Secure disposal	Potential
1.11	Scheme of delegation and terms of reference for committees		Until superseded or whilst relevant	Standard disposal	No
1.12	Meetings schedule		Current year	Standard disposal	No
1.13	Records relating to the election of chair and vice chair		Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	Secure disposal	Yes
1.14	Minutes of local academy board meetings	Section 248 of the Companies Act 2006	Date of report + 10 years	Secure disposal	Yes
1.15	All records relating to the conversion of a school to Dixons Academies Trust		For the life of the trust		Potential
1.16	Records relating to complaints made to and investigated by the accounting officer / principal or board of trustees / local academy board		Major complaints: current year + 6 years Negligence: current year + 15 years Child protection or safeguarding issue: current year + 40 years		
1.17	Correspondence sent and received by the board of trustees / local academy board or principal		Current year + 3 years	Secure disposal	Yes
1.18	Action plans created and administered by the board of trustees and / or its committees		Until superseded or whilst relevant	Secure disposal	No

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
1.19	Policies created and administered by the board of trustees		Until superseded	Standard disposal	No
1.20	Records relating to the appointment of the governance professional		Date on which governance professional appointment ceases + 6 years	Secure disposal	Yes
1.21	Records relating to the terms of office of serving trustees and ambassadors including evidence of appointment		Date of appointment ceases + 6 years	Secure disposal	Yes
1.22	Records relating to trustee and ambassador declaration against disqualification criteria		Date appointment ceases + 6 years	Secure disposal	Yes
1.23	Register of business interests		Date appointment ceases + 6 years	Secure disposal	Yes
1.24	Governance code of conduct		This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation	Standard disposal	No
1.25	Records relating to the training required and received by trustees		Date trustee steps down + 6 years	Secure disposal	Yes
1.26	Records relating to the induction programme of new trustees and ambassadors		Date of appointment ceases + 6 years	Secure disposal	Yes
1.27	Records relating to DBS checks carried out on members, trustees and ambassadors		Date of DBS check + 6 months	Secure disposal	Yes
1.28	Privacy notices		Until superseded + 6 years	Standard disposal	
2	**Management of an academy**				
2.1	Minutes of senior management team meetings and the meetings of other internal administrative bodies		Date of the meeting + 3 years (then review)	Secure disposal	Potential
2.2	Reports created by the principal or the management team		Date of the report + a minimum of 3 years then review annually or as required. If not, destroyed	Secure disposal	Potential
2.2	Reports created by the principal or the management team		Date of the report + a minimum of 3 years then review annually or as required. If not, destroyed	Secure disposal	Potential
2.3	Records, created by principal, senior leaders and other staff with administration responsibilities which do not fall under any other category		Current academic year + 6 years then review annually, or as required. If not, destroyed	Secure disposal	Potential
2.4	Correspondence created by principals, senior leaders and administration staff		Current year + 3 years	Secure disposal	Potential
2.5	Professional development plans		These should be held on the individual's HR record. If not, then termination of employment + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
2.6	General file series which do not fit under any other category		Current year + 5 years, then review	Secure disposal	Potential
2.7	Records relating to the creation and publication of the school brochure or prospectus		Current academic year + 3 years	The school could preserve a copy for their archive otherwise standard disposal	No
2.8	Records relating to the creation and distribution of circulars to staff, parents or students		Current academic year + 1 year	Standard disposal	No
2.9	Consent relating to school activities as part of data protection compliance		Consent will last whilst the student attends school and destroyed when the student leaves	Secure disposal	Yes
2.10	Newsletters and other items with a short operational use.		Current academic year + 1 year (academies may decide to archive one copy)	Standard disposal	No
2.11	Visitor management systems		Last entry in the 'visitors book' + 6 years (in case of claims)	Secure disposal	Yes
	School trips				
2.12	Parental consent forms for school trips where there has been no major incident		Although the consent forms could be retained from date of birth + 22 years, the school may wish to complete a risk assessment to assess whether the forms are likely to be required and could make a decision to dispose of the consent form at the end of the trip (or at the end of the academic year)	Secure disposal	Yes
2.13	Parental consent forms for school trips where there ***has been a major incident***		Date of birth of the student involved +25 years. The consent forms for all students on the trip need to be retained to show that the rules had been followed for all students	Secure disposal	Yes
3	**Student's education record**				
3.1	Student's educational record: Primary	Student's educational record required by The Education (Student Information) (England) Regulations 2005	Retain whilst the child remains at primary school	The file should follow the student when he / she leaves the primary school. This will include: • to another primary school • to a secondary school • to a student referral unit	Yes
3.2	Student's educational record: Secondary	Student's educational record required by The Education (Pupil Information) (England) Regulations 2005	Date of birth of the student + 25 years	Review	Yes
3.3	Student examination results (student copies)		This information should be added to the student file	All uncollected certificates should be returned to the examination board after reasonable attempts to contact the student have failed	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
3.4	Internal examination results		The information should be added to the student file	In line with a student's file (see clause 3.1 and 3.2)	Yes
3.5	Child protection information held on student file	Keeping children safe in education statutory guidance Working together to safeguard children A guide to inter-agency working to safeguarding and promote the welfare of children 2018	If any records relating to child protection issues are placed on the student file, it should be in a sealed envelope and then retained for the same period of time as the student file	If any records relating to child protection issues are placed on the student file, it should be in a sealed envelope and then retained for the same period of time as the student file	Yes
3.6	Child protection information held in separate files	Keeping Children Safe in Education statutory guidance Working together to safeguard children	Date of birth of student + 25 years then review	Secure disposal	Yes
3.7	Attendance registers	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made	Secure disposal	Yes
3.8	Correspondence relating to any absence (authorised or unauthorised)	Education Act 1996 Section 7	Current academic year + 2 years	Secure disposal	Potential
3.9	Special educational needs files, reviews and education, health and care plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Children and Family's Act 2014 Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the student + 31 years (Education Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act	Secure disposal	Yes
	Statistics and management information				
3.10	Examination results (school's copy)		Current year + 6 years	Secure disposal	Yes
3.11	SATS records: results		The SATs results should be recorded on the student's educational file and will therefore be retained until the student reaches the age of 25 years. The school may wish to keep a composite record of all of the whole year's SATS results. These are kept for the current year + 6 years to allow suitable comparison	Secure disposal	Yes
3.12	SATS records: examination papers		The examination papers should be kept until any appeals / validation process is complete.	Secure disposal	Yes
3.13	Published admissions number (PAN) reports Liaison with external agencies (family liaison, local authority, central government)		Current year + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
	Liaison with external agencies (family liaison, local authority, central government)				
3.14	Reports from outside agencies where the report has been included on the case file created by the outside agency		Whilst the student is attending the school then destroy	Secure disposal	Yes
3.15	Referral forms		While the referral is current	Secure disposal	Yes
3.16	Contact data sheets		Current year then review. If contact is no longer active then destroy	Secure disposal	Yes
3.17	Contact data base entries		Current year then review. If contact is no longer active then destroy	Secure disposal	Yes
3.18	Secondary transfer sheets (primary)		Current year + 2 years	Secure disposal	Yes
3.19	Attendance returns		Current year + 1 year	Secure disposal	Yes
3.20	School census returns		Current year + 5 years	Secure disposal	No
3.21	Ofsted reports and papers where a physical copy is held		Life of the report then review	Secure disposal	No
3.22	Returns made to central government		Current year + 6 years	Secure disposal	No
3.23	Circulars and other information sent from central government		Operational use	Secure disposal	No
	Admissions				
3.24	All records relating to the creation and implementation of the admissions policy	School admissions code statutory guidance for admissions authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels October 2022	Life of the policy + 3 years then review	Secure disposal	No
3.25	Admissions – if the appeal is unsuccessful	School admissions code statutory guidance for admissions authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels October 2022	Resolution of the case + 1 year	Secure disposal	Yes
3.26	Register of admissions	School admissions code statutory guidance for admissions authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels October 2022	Every entry in the 'admissions register' must be preserved for a period of three years after the date on which the entry was made		Yes
3.27	Proof of address supplied by parents as part of the admissions process		Current year + 1 year	Secure disposal	Yes
3.28	Supplementary information form		Current year + 1 year	Secure disposal	Yes
3.29	For successful admissions		The information to be added to the student file	See item	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
3.30	For unsuccessful admissions		Until appeals process has been completed	Secure disposal	Yes
4	**Human resources (management of personnel records)**				
4.1	All records leading up to the appointment of a principal		Unsuccessful: date of application + 6 months	Secure disposal	Yes
4.2	All records leading up to the appointment of a member of staff – unsuccessful candidates		Date of application + 6 months	Secure disposal	Yes
4.3	Pre-employment vetting checks for successful candidates	Current version of Keeping Children Safe in Education	Application forms, references and other documents – for the duration of the employee's employment + 6 years	Secure disposal	Yes
4.4	Pre-employment vetting checks for successful candidates (DBS checks)	DBS checks: guidance for employers	Copies of proof of identity: only kept for the purpose for which it was obtained. Destroyed after 6 months	Secure disposal	Yes
4.5	Pre-employment vetting information – evidence proving the right to work in the United Kingdom – successful candidates	An Employer's Guide to Right to Work checks (18 Oct 2023)	Where possible, these documents should be added to the staff HR file but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment + not less than 2 years	Secure disposal	Yes
4.6	Staff personnel file	Limitation Act 1980 (Section 2)	Termination of employment + 6 years	Secure disposal	Yes
4.7	Sickness absence monitoring	Statutory Sick Pay (SSP) employer guide	Current year + 3 years. We do not need to keep records of statutory sick pay (SSP) paid to employees, but HMRC may need these records if there is a dispute over payment of SSP.	Secure disposal	Yes
4.8	Staff training records – where training leads to continuing professional development		Length of time required by the professional body	Secure disposal	Yes
4.9	Staff training – except where dealing with children (e.g. first aid or health and safety)		Retained with the personnel file (see item 3.6)	Secure disposal	Yes
4.10	Staff training – where the training relates to children (e.g. safeguarding or other child related training)		Date of training + 40 years	Secure disposal	Yes
4.11	Time sheets		Current academic year + 6 years	Secure disposal	Yes
	Human resources (disciplinary and grievance processes)				
4.12	Records relating to any allegation of a child protection nature against a member of staff	Current version of Keeping Children Safe in Education	Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer), then review. Note: allegations that are found to be malicious should be removed from personnel files.	Secure disposal (shredded)	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
4.13	Disciplinary proceedings: (note in appendix 3)	ACAS code of practice. See note in appendix 3			Yes
	Oral warning		Date of warning + 6 months	Secure disposal	
	Written warning – level 1		Date of warning + 6 months		
	Written warning – level 2		Date of warning + 12 months		
	Final warning		Date of warning + 18 months		
	Case not found		If the incident is related to child protection, then see note in appendix 3. Otherwise, dispose of at the conclusion of the case	Secure disposal	Yes
	Human resources (payroll and pensions)				
4.14	Absence record		Current year + 3 years	Secure disposal	Yes
4.15	Batches	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6	Secure disposal	Yes
4.16	Car allowance claims	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 3 years	Secure disposal	Yes
4.17	Elements		Current year + 2 years	Secure disposal	Yes
4.18	Income tax form P60		Current year + 6 years	Secure disposal	Yes
4.19	Insurance	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.20	Maternity payment		Current year + 3 years	Secure disposal	Yes
4.21	National insurance – schedule of payments	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.22	Overtime		Current year + 3 years	Secure disposal	Yes
4.23	Payroll – gross / net weekly or monthly	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.24	Payroll reports	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.25	Payslips – copies	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.26	Pension payroll	Taxes Management Act 1970 income and corporation taxes 1988	Current year + 6 years	Secure disposal	Yes
4.27	Personal bank details	If employment ceases, then end of employment + 6 ears	Until superseded + 3 years	Secure disposal	Yes
4.28	Sickness records		Current year + 3 years	Secure disposal	Yes
4.29	Staff returns		Current year + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
4.30	Tax forms P6 / P11 / P11D / P35 / P45 / P46 / P48		Current year + 6 years	Secure disposal	Yes
5	**Health and safety**				
5.1	Health and safety policy statements		Life of policy + 3 years	Secure disposal	No
5.2	Health and safety risk assessments		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Secure disposal	Potential
5.3	Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Social Security (claims and payments) Regulations 1979. Regulation 25 Social Security Administration Act 1992 Section 8 Limitation Act 1980	The Accident Book (BI 510) 3 years after last entry in the book. Completed pages must be kept secure with restricted access.	Secure disposal	Yes
5.4	Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Social Security (claims and payments) Regulations 1979. Regulation 25 Social Security Administration Act 1992 Section 8 Limitation Act 1980	The Accident Book (BI 510) 3 years after last entry in the book. Completed pages must be kept secure with restricted access.	Secure disposal	Yes
5.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12 (2)	Date of incident + 3 years providing that all records relating to the incident are held on the HR file. The incident report must be kept secure with restricted access	Secure disposal	Yes
5.6	Control of Substances Hazardous to Health (COSHH)	Control of Substances Hazardous to Health Regulations 2002 SI 2002 No 2677 Regulations 11.	Date of incident + 40 years	Secure disposal	Yes
5.7	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	Secure disposal	Potential

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
5.8	Process of monitoring areas where employees and persons are likely to have come into contact with radiation. Maintenance records or controls, safety features and PPE. Dose assessment and recording	The Ionising Radiation Regulation 2017. SI 2017 No 1075 Regulation 11 As amended by SI 2018 No 390 Personal Protective Equipment (enforcing) Regulations 2018	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination For the dose assessment and recording, to keep the records made and maintained until the person to whom the record relates has or would have attained the age of 75 years, but in any event for at least 30 years from when the record was made	Secure disposal	Potential
5.9	Fire precautions log books		Current year + 3 years	Secure disposal	No
5.10	Health and safety file to show current state of buildings, including all alterations to be passed on in the case of change of ownership		Pass to new owner on sale or transfer of building	Secure disposal	No
6	**Financial management**				
6.1	Employer's liability insurance certificate		Closure of the company + 40 years (may be kept electronically)	Secure disposal	No
6.2	Inventories of furniture and equipment		Current year + 6 years	Secure disposal	No
6.3	Burglary, theft and vandalism report forms		Current year + 6 years	Secure disposal	Potential
6.4	Annual accounts		Current year + 6 years	Standard disposal	No
6.5	All records relating to the creation and management of budgets, including the annual budget statement and background papers		Life of the budget + 3 years	Secure disposal	No
6.6	Invoices, receipts, order books and requisitions, delivery notices		Current financial year + 6 years	Secure disposal	No
6.7	Records relating to the collection and banking of monies		Current financial year + 6 years	Secure disposal	No
6.8	Records relating to the identification and collection of debt		Final payment of debt + 6 years	Secure disposal	No
6.9	Student grant applications		Current year + 3 years	Security disposal	Yes
6.10	Pupil premium fund records		Date student leaves the provision + 6 years	Secure disposal	Yes
6.11	All records relating to the management of contracts under seal	Limitation Act 1080	Last payment on the contract + 12 years	Secure disposal	No
6.12	All records relating to the management of contracts under signature	Limitation Act 1080	Last payment on the contract + 6 years	Secure disposal	No
6.13	Records relating to the monitoring of contracts		Life of contract + 6 or 12 years	Secure disposal	No
6.14	Free school meals registers (where the register is used as a basis for funding)		Current year + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions / guidance	Retention period	Action at the end of the administrative life of the record	Personal information
6.15	School meals registers		Current year + 3 years	Secure disposal	Yes
6.16	School meals summary sheets		Current year + 3 years	Secure disposal	Yes
7	**Property management and maintenance**				
7.1	Title deeds of the properties belonging to the academy		These should follow the property unless the property has been registered with the Land Registry		No
7.2	Plans of the property belonging to the academy		These should be retained whilst the building belongs to the academy and should be passed on to any new owners if the building is lease or sold.		No
7.3	Leases of property leased by or to the academy		Expiry of lease +6 years		No
7.4	Records relating to the letting of school premises		Current financial year +6 years		No
7.5	All records relating to the maintenance of the academy carried out by contractors		These should be retained whilst the building belongs to the academy and should be passed on to any new owners if the building is leased or sold		Potential
7.6	All records relating to the maintenance of the academy carried out by school employees, including maintenance log books		These should be retained whilst the building belongs to the academy and should be passed on to any new owners if the building is leased or sold		Potential

Appendix 2

Information classification and data handling

Level	Definition	Key security requirement	Examples	Storage	Dissemination and access	Exchange and collaboration
Personal	Non-business data, for personal use only	No trust requirement				
Public	Trust information that is specifically prepared and approved for public consumption This information which does not require protection and is considered 'open' or 'unclassified' and which may be seen by anyone whether directly linked with our trust or not	**Availability** This information should be accessible to our trust whilst it is required for business purposes Back up requirements will need to be considered in relation to the importance of the information.	Prospectus, programme and course information Press release (not under embargo) Open content on trust website Flyers and publicity leaflets Published information released under the Freedom of Information Act Policies once they are approved Annual report and financial statements	Electronic information should be stored using our trust's provided IT facilities to ensure appropriate management, back up and access	Information can be shared via the web without requiring a Dixons Academies trust username Electronic and hard copy information can be circulated freely subject to applicable laws, e.g. copyright, contract, competition May be accessed remotely and via portable and mobile devices without encryption	Information can be exchanged via email or file sharing without needing encryption
Restricted	Non-confidential information where dissemination is restricted in some way (e.g. to members of our trust, partners, suppliers or affiliates). Access to this information enhances trust operations by facilitating communication and collaboration between staff, students and external partners, but access is restricted and governed by appropriate policies or contracts The documents may be restricted to our trust, or to a group in it, or to a group in our trust and an external partner	**Availability** This information should be accessible to the trust whilst it is required for business purposes Back up requirements will need to be considered in relation to the importance of the information	Some committee minutes Departmental intranets Trust timetable On-line directory of contact details Teaching materials Procurement documents Internal briefing papers	Electronic and paper-based information must be stored using our trust's provided facilities	Information can be shared via the web, but the user must provide DAT authentication or a federated authentication Electronic and hard copy information can be circulated on a need-to-know basis to trust members subject to applicable laws and trust regulations	Information can be sent in unencrypted format via email Information can be shared using DAT IT facilities e.g. OneDrive, SharePoint, shared file store

Level	Definition	Key security requirement	Examples	Storage	Dissemination and access	Exchange and collaboration
Confidential	Information which is sensitive in some way because it may be personal data, commercial or legal information, or be under embargo prior to wider release **The data has the potential to cause a negative impact on individuals' or our trust's interests (but not falling into highly confidential).** It also includes information in a form that could not be disclosed under freedom of information legislation. Covers data about an individual and data about the institution. This information, if compromised, could: • cause damage or distress to individuals • breach undertakings to maintain the confidence of information provided by third parties • breach statutory restrictions or the use of disclosure of information or lead to a fine • breach contractual agreements • breach duty of confidentiality or care • cause financial loss or loss of earning potential to our trust • disadvantage our trust in commercial or policy negotiations with others • Prejudice the investigation or facilitate the commission of a crime • Undermine the proper management of our trust and its operations	**Confidentiality and integrity** The information requires security measures, controlled and limited access and protection from corruption. Back up requirements will need to be considered in relation to the importance of the information.	Data contains private information about living individuals and it is possible to identify those individuals (e.g. salaries, student assessment marks) • Non-public data relates to business activity and has potential to affect financial interests and or elements of our trust's reputation (e.g. tender bids prior to award of contract, exam questions prior to use) • Non-public information that facilitates the protection of our trust's assets in general, (e.g. access codes for lower risk areas) Internal reports Commercial contracts Data related to living individuals, whether employees of our trust or not Data that is commercially sensitive to a project or a company providing research funds	Information must be stored using DAT IT facilities. Portable devices must have full disk encryption **USB sticks must not be used** Encrypted removable media is not permitted without undertaking evaluation of other options	Access to confidential data must be strictly controlled by the data owner who should conduct regular reviews Some types of confidential information may be shared with authorised users via DAT IT facilities **Confidential data must not be extracted from our trust's IT systems and stored on local IT systems**	The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected **Confidential data must be encrypted** Exchange must be conducted using DAT provided facilities Duplicate copies of confidential information must be avoided. Where copies are necessary, the protective marking must be carried with the data copies and are required for circulation or sharing, secure delivery methods must be used Paper and electronic copies must be marked 'confidential' and the intended recipients clearly indicated Printed copy should be disposed of in accordance with the retention schedule

Level	Definition	Key security requirement	Examples	Storage	Dissemination and access	Exchange and collaboration
Highly confidential	Information which is sensitive and has the potential to cause serious damage or distress to individuals or serious damage to our trust's interests if disclosed inappropriately Data contains highly sensitive private information about living individuals and it is possible to identify those individuals Non-public data. Relates to business activity and has the potential to seriously affect commercial interests and / or our trust's corporate reputation	**Confidentiality and integrity** This information requires significant security measures, strictly controlled and limited access and protection from corruption Back up requirements will need to be considered in relation to the importance of the information	Student personal details Staff personal details Financial transactions Research data Medical records Serious disciplinary matters Papers relating to possible redundancies	Information must be stored using DAT IT facilities. Portable devices must have full disk encryption **USB sticks must not be used** Encrypted removable media is not permitted without undertaking evaluation of other options Storage on personally owned computer is NOT permitted	Access to confidential data must be strictly controlled by the data owner who should conduct regular reviews. Some types of confidential information may be shared with authorised users via DAT IT facilities **Confidential data must not be extracted from our trust's IT systems and stored on local IT systems**	The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected **Confidential data must be encrypted** Exchange must be conducted using DAT provided facilities Duplicate where paper copies of confidential information must be avoided. Where copies are necessary, the protective marking must be carried with the data copies and are required for circulation or sharing, secure delivery methods must be used Paper and electronic copies must be marked 'confidential' and the intended recipients clearly indicated Printed copy should be disposed of in accordance with the retention schedule

Appendix 3

Disciplinary hearings – guidance notes

The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period.

Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line, and defend him-or-herself by saying 'I would never do something like that', reference to the early proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that he or she had 'fifteen years of unblemished service', the record of the disciplinary proceedings would be effective evidence to counter this claim.

Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be 'removed from the file'. This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.