# Information Management Toolkit for Schools

August 2018

**Contents**

## 1. Introduction

The Information Management Toolkit for Schools has been created to assist schools in their compliance with the Freedom of Information Act 2000, the Data Protection Act 2018 and the General Data Protection Regulations 2016.

Wherever the Toolkit (or other guidance issued by external bodies) refers to a "school" this refers to local authority schools. Whilst some of the information in this toolkit will be relevant for Academies. There is separate guidance available for Academies/

Although the Lord Chancellor's Code talks about records management, this Toolkit has been entitled Information Management Toolkit for Schools to make it clear that this covers all the information which a school might create and manage rather than just "records".

To access the different parts of the Toolkit please click on the relevant section in the table of contents and the hyperlink will take you to the right place in the document.

If you have any comments to make about the Information Management Toolkit for Schools, or would like to suggest any additions, please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk or 03000 415812.

## 2. Scope

The Information Management Toolkit aims to assist individual schools in managing records throughout their lifecycle and to ensure compliance with the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000.

The Toolkit also aims to assist individual schools to put the relevant records management policy/programme in place for compliance with the Data Protection Act 2018 and the General Data Protection Regulations 2016.

## 3. Records Management Policy

Under section 7 of the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000:

*Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy.*

*3.1 The policy should be endorsed by senior management, for example at board level, and should be readily available to staff at all levels.*

*3.2 The policy provides a mandate for the records and information management function and a framework for supporting standards, procedures and guidelines. The precise contents will depend on the particular needs and culture of the school but it should as a minimum:*

*a) Set out the school's commitment to create, keep and manage records which document its principal activities;*
*b) Outline the role of records management and its relationship to the school's overall business strategy;*
*c) Identify and make appropriate connections to related policies, such as those dealing with email, information security and data protection;*
*d) Define roles and responsibilities, including the responsibility of individuals to document*

*their work in the school's records to the extent that, and in the way that, the school has decided their work should be documented, and to use those records appropriately;*

*e) Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored.*

*3.3 The policy should be kept up-to-date so that it reflects the current needs of the school. One way of ensuring this is to review it at agreed intervals, for example every three or five years, and after major organisational or technological changes, in order to assess whether it needs amendment.*

*3.4 The school should consider publishing the policy so that members of the public can see the basis on which it manages its records.*

[For a full copy of the Lord Chancellor's Code of Practice see http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

See Appendix A for the model Records Management Policy.

The model policy statement can be adopted in its entirety or can be amended to reflect the needs of individual schools. Once it has been amended it should be approved by the governing body or other appropriate senior management team. Once the records management policy has been approved at the appropriate level it should be published, perhaps as part of the publication scheme.

## 4. Organisational arrangements to support information management

Section 6 of the Lord Chancellor's Code requires authorities to have in place organisational arrangements which support records management. A summary of what appears in section 6 of the Code is listed below. However, a small school will not need to have the same numbers of people involved as a large school and a number of roles may be pulled together and managed by one member of staff.

**4.1** Recognition of records management as a core corporate function, either separately or as part of a wider information or knowledge management function. The function should cover records in all formats throughout their lifecycle, from planning and creation through to disposal and should include records managed on behalf of the authority by an external body such as a contractor;

**4.2** Inclusion of records and information management in the school's risk management framework. Information and records are a corporate asset and loss of the asset could cause disruption to business. The level of risk will vary according to the strategic and operational value of the asset to the school and risk management should reflect the probable extent of disruption and resulting damage;

**4.3** A governance framework that includes defined roles and lines of responsibility. This should include allocation of lead responsibility for the records and information management function to a designated member of staff at sufficiently senior level to act as a records management champion, and allocation of operational responsibility to a member of staff with the necessary knowledge and skills. In schools, it may be more practicable to combine these roles. Ideally the same people will be responsible also for compliance with other information legislation, for example the Data Protection Act 2018, General Data Protection Regulations 2018 and the Re-use of Public Sector Information Regulations 2005, or will work closely with those people;

**4.4** Clearly defined instructions, applying to staff at all levels in the school, to create, keep and manage records.

**4.5** Identification of information and business systems that hold records and provision of the resources needed to maintain and protect the integrity of those systems and the information they contain;

**4.6** Consideration of records management issues when planning or implementing ICT systems, when extending staff access to new technologies and during re-structuring or major changes to the authority;

**4.7** Induction and other training to ensure that all staff are aware of the school's records management policies, standards, procedures and guidelines and understand their personal responsibilities. This should be extended to temporary staff, contractors and consultants who are undertaking work that it has been decided should be documented in the school's records.

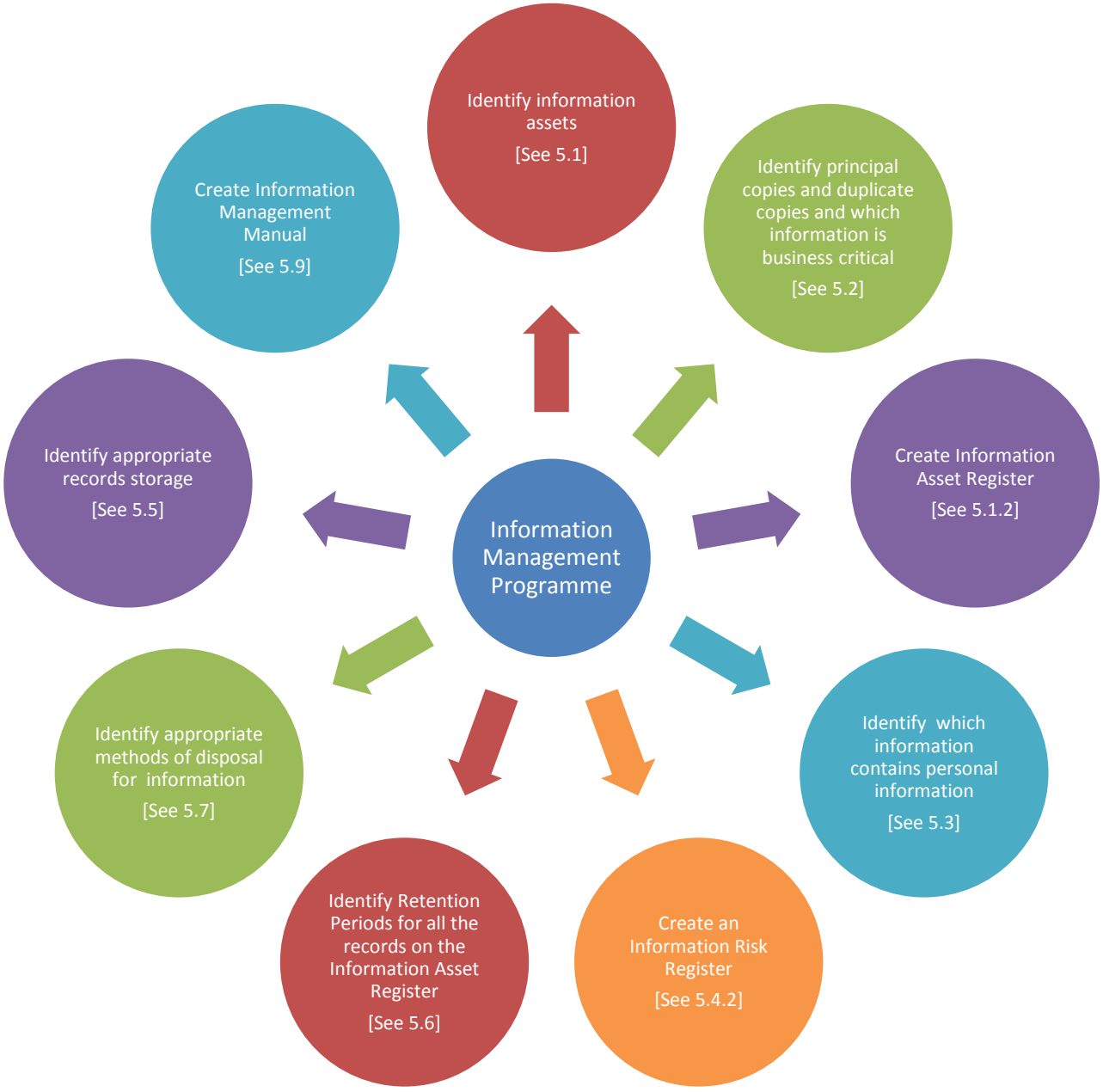
**4.8** An agreed programme for managing records in accordance with this part of the Code;

**4.9** Provision of the financial and other resources required to achieve agreed objectives in the records management programme.

## 5. Information Management Programme

The school should develop an information management programme which ensures that all the information which the school creates, holds and manages is reliable, authentic, accurate and usable.

The information management programme should contain the following elements which are dealt with in more detail below.



## 5.1 Identifying Information Assets

The first step in an effective information management programme is to identify the different information assets which the school holds. These will vary depending on the size of the school, but are likely to include pupil records, financial information, building maintenance information, employee records, amongst other things which can be found in the retention schedule in section 5.6.

Some schools will already have a list of records which the school holds and others will have no idea about what records are held and where they are. In the latter case it may be necessary to undertake an information asset survey (also known as an information audit).

### 5.1.1 Information Audits

Information audits are recommended under section 10.2 of the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000.

> *Authorities should gather and maintain data on records and information assets. This can be done in various ways, for example through surveys or audits of the records and information held by the school. It should be held in an accessible format and should be kept up to date.*

The key to an effective information audit is to understand why the information is being created as this is the framework on which everything else will be based.

The information audit needs to establish the following information:

- A description of the information asset;
- The information asset owner;
- Whether or not the information asset is a principal copy;
- The format the information asset is held in and where it is held;
- Where appropriate, the statutory purpose for the creation of the information asset including any workflow diagrams;
- Whether the information asset is a core/business critical record;
- How long the information asset needs to be retained and how it should be archived;
- Methods of disposing of the information asset;
- Whether the information asset contains any personal or other sensitive information.

Information audits can be completed by face to face conversations with different record holders or by using a questionnaire method.

A questionnaire can be a good way of establishing which records each individual member of staff thinks that they are responsible for and for identifying duplicate records.

The amount of time and resource required to complete an information audit will depend on the size of the school and the number of records which are created.

For further information about how to set up an information asset survey please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk.

### 5.1.2 Information Asset Register

An information asset register is a register of unpublished information holdings i.e. information or collections of information, held electronically or in hard copy which will usually not have been published or made publicly available.

The information asset register does not provide direct access to the information holdings themselves.

Schools are not required to have an information asset register; however, it is a useful exercise to create a list of all the information assets identified in the information audit. This can be especially useful in larger schools where there may be a greater number of information assets.

The school may also wish to use the retention schedule as an information asset register as this is the other place where all the information assets will be listed. Additional columns can be added to the retention schedule to create an information asset register.

The information asset register should contain the following information:

- Description of the information asset;
- Information asset owner/ Information asset manager [these could be the same person];
- Whether the information is a principal copy;
- The name of the principal record keeper;
- Whether the information is business critical;
- The retention period;
- The protective marking.

The information asset register can be used to record the Records of Processing Activities under Article 30 of the General Data Protection Regulations 2016. Further information and a template can be found on the Information Commissioner's website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

## 5.2 Principal and Duplicate Copies

### 5.2.1 Principal Copies

Principal copies of information consist of the master set of documents which will make up the record of any transaction in the school. Groups of documents will include contract documentation, project documentation, financial records, personnel records, records of meetings amongst others.

The principal copy of any information will be the one used to protect the school's liability in any future legal action or complaint or to support service delivery.

### 5.2.2 Principal Record Keepers

The person or team who holds the principal copy of the information is called the principal record keeper (in other words they are holding the information which records the activity). It is the responsibility of the Principal Record Keeper to ensure that the "principal" record is managed properly in line with the retention periods laid out in the school's retention schedule [See Section 5.6].

If a principal record keeper is not identified then there will always be confusion about which copy of the information is the principal copy. Where this confusion exists usually either all the copies of

the information are kept (which means that the school is storing more information than it requires) or that all the copies of the information are destroyed (which means that the school could be vulnerable to legal challenge in the future).

It is the responsibility of the principal record keeper to ensure that the information is transferred if the post-holder is replaced or if a restructure takes place. This should ensure that information is not "lost" when a restructure takes place or the post holder moves on.

Most members of staff will hold some principal copies and some duplicate records.

### 5.2.3 Business Critical Information

It is important to identify information which is business critical so that resources are not wasted on managing information which is not critical to the business function (or which could be replaced relatively easily from other sources). It is also important to distinguish between business critical records and non-business critical records for business continuity purposes.

It is strongly recommended that individual managers create and maintain a register of the business critical information in the school, the responsible member of staff and its location. This information can then be used as the basis for a salvage plan.

**DEFINITION:**
*Business critical information is the information without which the school cannot continue its business. It is probable that these will be the principal copies of information which could not be replaced if they were to be lost or damaged. Loss of the information could result in serious consequences either in the loss of life or in the school's inability to fulfil its statutory obligations or in the school's inability to defend itself in a legal case. The loss of the information could also lead to serious reputational damage.*

### 5.2.4 Non Business Critical Information

These records are usually copies or duplicates of principal information or information which has an administrative or operational use but which could be replaced if it was lost or damaged.

### 5.2.5 Duplicate Copies

Duplicate information is the information which individual members of staff retain for operational purposes (for example, minutes of meetings attended or copies of reports presented to meetings, agendas, reference material and so on). This information is usually managed outside of the principal filing system.

Duplicate information is also subject to disclosure under the Freedom of Information Act 2000 and the Environmental Information Regulations 1992. The retention of duplicate information may also constitute a breach of the Data Protection Act 2018 or the General Data Protection Regulations 2016.

Duplicate and operational copies can and should be safely disposed of once they have reached the end of their operational use in line with the appropriate disposal requirements for their protective marking category [see Section 5.3 below].

## 5.3 Identifying and Marking Confidential Information

Schools do not need to have a protective marking scheme, however, identifying and marking records which contain sensitive information can be useful. The protective marking can be recorded

in the Information Asset Register and will give members of staff an indication of how sensitive records are.

A possible protective marking scheme could be as follows:

**NOT PROTECTIVELY MARKED**
All information which could be disclosed
**OFFICIAL**
All information which is politically and commercially sensitive
**OFFICIAL SENSITIVE**
All information which contains personal/sensitive personal data

The protective marking categories which have been assigned to records in the retention schedule have been developed using this scheme.

## 5.4 Managing Information Risk

### 5.4.1 Assessing Information Risk

Assessing information risk is very similar to other forms of risk assessment. Information risk assessment needs to cover:

- whether the information is a principal copy;
- whether the information is business critical;
- what the consequences would be if the information was lost, stolen or damaged including damage to individuals and reputational damage;
- how easy the information would be to replace;
- where the information is stored (e.g. is personally sensitive information stored in locked cabinets to avoid theft).

Once this process has been completed, each information asset can be assigned an information risk category. The school can then look at how high risk information can be protected (for example, personally sensitive information should not be carried on an unencrypted data stick) and the likelihood of information being lost or stolen can be reduced.

### 5.4.2 Information Risk Register

All this information can be recorded in an information risk register so it is clear, if high risk data is lost or stolen, that the appropriate steps have been taken to safeguard the information. If appropriate, an additional column can be added to the retention schedule.

## 5.5 Appropriate Records Storage

Records (whether physical or electronic) must be managed to ensure that they cannot be lost, damaged or destroyed. This will usually involve the purchase of high quality storage equipment. It may not always be necessary to store non-core records in the same high quality storage.

### 5.5.1 Physical Records

Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured against intruders and have controlled access as far as possible to the working space.

The following are hazards which need to be considered before approving areas where physical records can be stored.

**Environmental Damage - Fire**

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but for important core records, fire proof cabinets may need to be considered. However, fireproof cabinets are expensive and very heavy so they should only be used in special circumstances.

Records which are stored on desks or in cupboards which do not have doors will suffer more damage than those which are stored in cupboards/cabinets which have close fitting doors.

**Environmental Damage - Water**

Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive, therefore, records need to be protected against water damage where possible. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground. Most office furniture stands 2 inches off the ground. Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that in the case of a flood that records are protected against immediate flood damage.

**Environmental Damage – Sunlight**

Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

**Environmental Damage - High Levels of Humidity**

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records often beyond repair.

The temperature in record storage areas should not exceed 18$^{o}$C and the relative humidity should be between 45% and 65%.

**Environmental Damage - Insect/Rodent Infestation**

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).

### 5.5.2 Electronic Records

Wherever possible, electronic records should be stored on network drives which are being backed up regularly. If appropriate, this could include stand-alone devices where the information is being regularly backed up.

Where possible portable devices, where information is held on the hard drive of the computer, should be encrypted.

Business critical records should not be stored on floppy disks or memory sticks as these media are not stable and digital information can become corrupted or lost.

CD/DVD may be used for short term storage of information but should be clearly labelled and locked away where appropriate. The CD/DVD should be checked routinely, at least once every six months, to ensure that the data is still accessible.

Records may be stored on external hard drives which should be encrypted where appropriate. This information should be backed up where appropriate or checked routinely, at least once every six months, to ensure that the data is still accessible.

## 5.6 Identifying Retention Periods for Information

### 5.6.1 The purpose of the retention schedule

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under both the Data Protection Act 2018, the General Data Protection Regulations 2018 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored. The retention periods referred to in the retention schedule below are minimum retention periods. Records can be kept for a longer period of time if necessary. However, staff do need to be aware that if a decision is made to keep a record for a longer period of time that they will still be disclosable under the Freedom of Information Act 2000.

### 5.6.2 Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

- Managing records against the retention schedule is deemed to be “normal processing” under the Data Protection Act 2018/General Data Protection Regulations 2016 and the Freedom of Information Act 2000.
- Members of staff can be confident about disposing of information at the appropriate time.
- Information which is subject to Freedom of Information and Data Protection legislation will be available when required.
- The school is not maintaining and storing information unnecessarily.
- The retention register can be expanded to include the information asset register and the

information risk register.

### 5.6.3 Useful Contacts

If you have a query about a retention period relating to a record series on the retention schedule or a query about the retention period for a record series which is not on the retention schedule then contact the Records Manager, Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk

### 5.6.4 Disposal of Records

All the records should be disposed of following the requirements laid out in section 5.7 below at the end of the retention period.

However, there may be some records which are of historical value. If you would like advice about how to manage historical records please contact Mark Bateson (Heritage Services Manager) at the Kent Library and History Centre; mark.bateson@kent.gov.uk. Records can be transferred to the Library and History Centre or can be kept in a record or archive room at the school.

### 5.6.5 Recommended Retention Periods

Where the Protective Marking column is blank, the record series should be considered to be “NOT PROTECTIVELY MARKED”

**IMTKS1 Governing Body**

For further information about governing body records please see: “The constitution of governing bodies of maintained schools Statutory guidance for governing bodies of maintained schools and local authorities in England August 2017”

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS1A** | **Management of Governing Body** | | | | | | | | | |
| IMTKS1A.1 | Instruments of Government | | Permanent | | | | YES | No | | |
| IMTKS1A.2 | Trusts and Endowments | | Permanent | | | | YES | No | | |
| IMTKS1A.3 | Records relating to the election of parent and staff governors not appointed by the governors | | Date of election + 6 months | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.4 | Records relating to the appointment of co-opted governors | | Provided that the decision has been recorded in the minutes the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.5 | 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 | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.6 | Scheme of Delegation and Terms of Reference for Committees | | PERMANENT | | | | YES | No | | |
| IMTKS1A.7 | Meetings Schedule | | Current year | | | | YES | No | | |
| IMTKS1A.8 | Agendas – Principal copy | The School Governance (Roles, Procedures and Allowances) (England) Regulations 2013 | Permanent | | | | YES | No | | |
| IMTKS1A.9 | Minutes - Principal set (signed) | As above | Permanent | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.10 | Reports made to the Governors’ Meeting which are referred to in the minutes | As above | Permanent | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.11 | Register of attendance at Full Governing Board meetings | As above | Date of last meeting in the book + 6 years | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.12 | Papers relating to the management of the Annual Parents’ Meeting | The Education (Annual Parents' Meetings) (England) Regulations 1999[1] | Date of meeting + 6 years | | | | YES | Yes | | |
| IMTKS1A.13 | Agendas – Additional Copies | | Date of meeting | | | | NO | No | | |
| IMTKS1A.14 | Minutes - Inspection copies | | Date of meeting + 3 years | | | | NO | Yes | | |

[1] Statutory Instruments 1999 No 2014

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS1A.15 | Records relating to Governor Monitoring Visits | | Date of the visit + 3 years | | | | YES | Yes | OFFICIAL | |
| IMTKS1A.16 | Annual Reports required by the Department for Education | Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI | Date of report + 10 years | | | | YES | No | | |
| IMTKS1A.17 | All records relating to the conversion of schools to Academy status | | PERMANENT | | | | YES | No | | |
| IMTKS1A.18 | Records relating to complaints made to and investigated by the Governing Body | | Date of resolution of complaint + 6 years then review for further retention in the case of contentious disputes | | | | YES | Yes | OFFICIAL SENSITIVE | |
| IMTKS1A.19 | Correspondence sent and received by the Governing Body | | Current year + 6 years | | | | YES | Yes | OFFICIAL | |
| **IMTKS1B** | **Management of Governors** | | | | | | | | | |
| IMTKS1B.1 | Records relating to the appointment of a clerk to the Governing Body | | Date appointment as clerk ceases + 6 years | | | | YES | Yes | OFFICIAL | |
| IMTKS1B.2 | Records relating to the terms of office of serving governors including evidence of appointment | | PERMANENT | | | | YES | Yes | OFFICIAL | |
| IMTKS1B.3 | Records relating to Governor Declaration against disqualification criteria | | Until the Governor steps down | | | | YES | Yes | OFFICIAL | |
| IMTKS1B.4 | Register of Business Interests | | PERMANENT | | | | YES | Yes | | |
| IMTKS1B.5 | Governors Code of Conduct | | This is expected to be a dynamic document, one copy of each version should be kept permanently | | | | YES | Yes | | |
| IMTKS1B.6 | Records relating to the training required and received by Governors | | Until the Governor steps down | | | | YES | Yes | OFFICIAL | |
| IMTKS1B.7 | Records relating to the induction programme for new governors | | Until the Governor steps down | | | | YES | Yes | OFFICIAL | |
| IMTKS1B.8 | Records relating to DBS checks carried out on clerk and members of the governing body | | Date of DBS check + 6 months | | | | YES | Yes | OFFICIAL | |

## IMTKS2 Pupil Management

| | | | | | Information Asset Register Information | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS2A** | **Admissions and Attendance** | | | | | | | | | |
| IMTKS2A.1 | Admission Registers | | Permanent | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.2 | Records relating to the admissions process – if the admission is successful | | Admission + 1 year | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.3 | Admissions – if the appeal is unsuccessful | | Resolution of case + 1 year | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.4 | Admissions – Secondary Schools – Casual | | Current year + 1 year | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.5 | Proofs of address supplied by parents as part of the admissions process | | Current year + 1 year | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.6 | Attendance registers | | Date of register + 3 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2A.7 | Letters authorising absence | | Date of absence + 2 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| **IMTKS2B** | **Pupil Educational Record** | | | | | | | | | |
| IMTKS2B.1 | Pupil Files and/or record cards - Primary | Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) | Retain for the time which the pupil remains at the Primary School<br>Transfer to the Secondary School (or other Primary School) when the child leaves the school[2] | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2B.2 | Pupil Files and/or record cards - Secondary | Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) | DOB of the pupil + 25 years[1] | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2B.3 | Examination results - Public | | Year of examinations + 6 years[3] | | | | No | Yes | | |
| IMTKS2B.4 | Examination results - Internal examination results | | Current year + 5 years<br>If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary | | | | No | Yes | | |
| IMTKS2B.5 | Any other records created in the course of contact with pupils | | Current year + 3 years then review | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2B.6 | Images held of pupils together with any consents and permissions to publish | | All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement | | | | Yes | Yes | OFFICIAL | |
| **IMTKS2C** | **Special Educational Needs** | | | | | | | | | |
| IMTKS2C.1 | Special Educational Needs files, reviews and Individual Education Plans | | DOB of the pupil + 25 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2C.2 | Statement maintained under The Education Act 1996 - Section 324 | Special Educational Needs and Disability Act 2001 Section 1 | DOB + 30 years<br>Unless legal action is pending | | | | Yes | Yes | OFFICIAL SENSITIVE | |

[2] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service. If the pupil has left the primary school and there is no information about which school that the pupil has moved onto, or they have moved onto elective home education, or the pupil has moved abroad or to an independent school, then the records can be sent to Elizabeth Barber, Room 2.89 Sessions House, Maidstone for archiving.

[3] Any certificates left unclaimed should be returned to the appropriate Examination Board

| | | | | | Information Asset Register Information | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS2C.3 | Proposed statement or amended statement | Special Educational Needs and Disability Act 2001 Section 1 | DOB + 30 years<br>Unless legal action is pending | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS2C.4 | Advice and information to parents regarding educational needs | Special Educational Needs and Disability Act 2001 Section 2 | Closure + 12 years<br>Unless legal action is pending | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS2C.5 | Accessibility Strategy | Special Educational Needs and Disability Act 2001 Section 14 | Closure + 12 years<br>Unless legal action is pending | | | | Yes | No | OFFICIAL SENSITIVE | |
| IMTKS2C.6 | Pupil SEN Files | | DOB of pupil + 25 years then review unless legal action is pending. If so, it may be appropriate to add an additional retention period. | | | | Yes | Yes | OFFICIAL SENSITIVE | |

## IMTKS3 School Trips and Extra Curricular Activities

| | | | | | Information Asset Register Information | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS3A** | **Educational Visits outside the Classroom** | | | | | | | | | |
| IMTKS3A.1 | Primary Schools Records created by schools to obtain approval to run an Educational Visit outside the Classroom[4] | 3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998) | Date of visit + 14 years[5] | | | | Yes | No | OFFICIAL SENSITIVE | |
| IMTKS3A.2 | Secondary Schools Records created by schools to obtain approval to run an Educational Visit outside the Classroom[3] | 3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998) | Date of visit + 10 years[4] | | | | Yes | No | OFFICIAL SENSITIVE | |
| **IMTKS3B** | **Day Trips** | | | | | | | | | |
| IMTKS3B.1 | Parental permission slips for school trips – where there has been no major incident | | Conclusion of the trip | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS3B.2 | Parental permission slips for school trips – where there has been a major incident | Limitation Act 1980 | DOB of the pupil involved in the incident + 25 years<br>The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| **IMTKS3C** | **Residential Trips** | | | | | | | | | |
| IMTKS3C.1 | All records relating to the organization of school residential trips | Limitation Act 1980 | Date of the residential visit + a minimum of 6 years then review | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| **IMTKS3D** | **Walking Bus** | | | | | | | | | |
| IMTKS3D.1 | Walking Bus registers | | Date of register + 3 years[6] | | | | Yes | Yes | OFFICIAL SENSITIVE | |

[4] including GOF1 and GOF2 and data entered on the e-go system
[5] This retention period has been set in agreement with the Safeguarding Children's Officer
[6] This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting

## IMTKS4 School Management – Teaching and Curriculum

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS4A** | **Senior Management Team** | | | | | | | | | |
| IMTKS4A.1 | Log Books | | Date of last entry in the book + 6 years | | | | Yes | No | | |
| IMTKS4A.2 | Minutes of the Senior Management Team and other internal administrative bodies | | Date of meeting + 5 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS4A.3 | Reports made by the Head Teacher or the management team | | Date of report + 3 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS4A.4 | Records created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities | | Closure of file + 6 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS4A.5 | Correspondence created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities | | Date of correspondence + 3 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS4A.6 | School development plans | | Closure + 6 years then review | | | | Yes | No | | |
| IMTKS4A.7 | Professional development plans | | Closure + 6 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS4A.8 | Action Plans | | Date of action plan + 3 years | | | | Yes | No | | |
| IMTKS4A.9 | Policy documents | | Expiry of policy<br>Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process) | | | | Yes | No | | |
| **IMTKS4B** | **Curriculum Management** | | | | | | | | | |
| IMTKS4B.1 | Timetable | | Current year then review | | | | No | No | | |
| IMTKS4B.2 | Curriculum development | | Current year + 6 years | | | | No | No | | |
| IMTKS4B.3 | Curriculum returns | | Current year + 3 years | | | | No | No | | |
| IMTKS4B.4 | School syllabus | | Current year then review | | | | No | No | | |
| IMTKS4B.5 | Schemes of work | | Current year then review | | | | No | No | | |
| IMTKS4B.6 | Class record books | | Current year then review | | | | No | No | | |
| IMTKS4B.7 | Mark Books | | Current year then review | | | | No | No | | |
| IMTKS4B.8 | Record of homework set | | Current year then review | | | | No | No | | |
| IMTKS4B.9 | Pupils' work | | Current year then review | | | | No | No | | |
| IMTKS4B.10 | SATS records including examination results. Exam papers should only be retained if they are required to evidence the results | | Current year + 6 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |

## IMTKS5 Management of Schools - Administration

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS5A** | **Personnel Management** | | | | | | | | | |

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS5A.1 | Employer's Liability certificate | | Closure of the school + 40 years | | | | Yes | | | |
| IMTKS5A.2 | Staff Personal files | | Termination + 6 years[7] | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.3 | Interview notes and recruitment records | | Date of interview + 6 months | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.4 | Pre-employment vetting information (including DBS checks)[8] | DBS guidelines | Date of check + 6 months | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.5 | Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure | | Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file. | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.6 | Right to Work in the UK checks | https://www.gov.uk/check-job-applicant-right-to-work | Termination of employment + 2 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.7 | Disciplinary proceedings: case not found | | Take advice from Personnel if the proceedings were child protection related otherwise destroy immediately at the conclusion of the case | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.8 | Disciplinary proceedings: written warnings | | The duration of the warning [9] | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.9 | Annual appraisal or assessment records | | Current year + 5 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5A.10 | Images held of members of staff together with any consents and permissions to publish | | All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement | | | | Yes | Yes | OFFICIAL | |
| **IMTKS5B** | **Health and Safety** | | | | | | | | | |
| IMTKS5B.1 | Policy Statements | | Date of expiry + 1 year<br>[it may be necessary to keep one copy of each policy so that a history of what policies were in place at any time] | | | | Yes | No | | |
| IMTKS5B.2 | Accessibility Plans | Disability Discrimination Act 1995 | Current year + 6 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5B.3 | Records relating to accident/injury at work | The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974 | Date of incident + 12 years [10] | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5B.4 | Accident Reporting – Children | Limitation Act 1980 | Date of birth + 22 years where the injured person is a minor at the time of the accident | | | | Yes | Yes | OFFICIAL SENSITIVE | |

[7] These files should be subject to KCC's open file policy where the employees are employed by Kent County Council as the Local Authority
[8] Please note that schools must not keep copies of the documents which are checked for DBS purposes.
[9] If this information has been added to an individual's personnel file, it must be weeded from the file once the retention period has elapsed
[10] In the case of serious accidents a further retention period will need to be applied

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS5B.5 | Accident Reporting – Adults | Social Security (Claims and Payments) Regulations 1979 Regulation 25.<br>Social Security Administration Act 1992 Section 8.<br>Limitation Act 1980 | Date of the accident + 4 years where the injured person is an adult at the time of the accident; | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5B.6 | Risk Assessments | The Management of Health & Safety at Work Regulations 1999<br>Health and Safety at Work Act 1974 | Current year + 3 years | | | | Yes | No | | |
| IMTKS5B.7 | COSHH Risk Assessments | Control of Substances Hazardous to Health (COSHH) Regulations 2002 | Date of creation + 40 years | | | | Yes | No | | |
| IMTKS5B.8 | Incident reports | | Current year + 20 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5B.9 | Process of monitoring areas where employees and persons are likely to have become in contact with asbestos | Control of Asbestos Regulations 2012 | Last action + 40 years | | | | Yes | No | | |
| IMTKS5B.10 | Process of monitoring of areas where employees and persons are likely to have come in contact with radiation | Ionising Radiations Regulations 2017 | Last action + 50 years | | | | Yes | No | | |
| IMTKS5B.11 | Fire Safety Records including Fire Safety Audits | Regulatory Reform (Fire Safety) Order 2005 | Current year + 6 years | | | | Yes | No | | |
| IMTKS5B.12 | Fire Risk Assessments | Regulatory Reform (Fire Safety) Order 2005 | Date the fire risk assessment expires + 6 years | | | | | | | |
| IMTKS5B.13 | Fire Drill records | Regulatory Reform (Fire Safety) Order 2005 | Date of fire drill + 6 years | | | | Yes | No | | |
| **IMTKS5C** | **Payroll and Pensions** | | | | | | | | | |
| IMTKS5C.1 | Records relating to the management of the payroll | HMRC - Compliance Handbook Manual CH15400 | Financial year to which the payroll is run + 6 years | | | | | | | |
| IMTKS5C.2 | Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Retirement Benefits Schemes (Information Powers) Regulations 1995 | Current year + 6 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5C.3 | Salary cards | | Last date of employment + 85 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5C.4 | Maternity pay records | Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567) | Current year + 3yrs | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5C.5 | Timesheets, sick pay | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| **IMTKS5D** | **Financial Records** | | | | | | | | | |
| IMTKS5D.1 | Annual Accounts | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | No | | |
| IMTKS5D.2 | Loans and grants | HMRC - Compliance Handbook Manual CH15400 | Date of last payment on loan + 12 years then review to see whether a further retention period is required | | | | Yes | No | NOT PROTECTIVELY MARKED | |
| IMTKS5D.3 | Inventories of equipment and furniture | | Current year + 6 years | | | | No | No | | |
| IMTKS5D.4 | Annual Budget and background papers | | Current year + 6 years | | | | Yes | No | | |

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS5D.5 | Budget reports, budget monitoring etc | | Current year + 3 years | | | | Yes | No | | |
| IMTKS5D.6 | Contracts - under seal | Limitation Act 1980 (Section 12) | Contract completion date + 12 years | | | | Yes | No | | |
| IMTKS5D.7 | Contracts - under signature | Limitation Act 1980 (Section 2) | Contract completion date + 6 years | | | | Yes | No | | |
| IMTKS5D.8 | Contracts - monitoring records | | Current year + 2 years | | | | Yes | No | | |
| IMTKS5D.9 | Order books and requisitions | | Current year + 6 years | | | | Yes | No | | |
| IMTKS5D.10 | Copy orders | | Current year + 2 years | | | | No | No | | |
| IMTKS5D.11 | Delivery Documentation | | Current year + 6 years | | | | Yes | No | | |
| IMTKS5D.12 | Invoice, receipts and other records covered by the HMRC - Compliance Handbook Manual CH15400 | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | No | | |
| IMTKS5D.13 | Petty cash books | HMRC - Compliance Handbook Manual CH15400 | Current financial year + 6 years | | | | Yes | No | | |
| IMTKS5D.14 | Debtors' Records | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | Yes | | |
| IMTKS5D.15 | Applications for free school meals, travel, uniforms etc | | Whilst child is at school | | | | No | Yes | OFFICIAL | |
| IMTKS5D.16 | Student grant applications | | Current year + 3 years | | | | Yes | Yes | OFFICIAL | |
| IMTKS5D.17 | School Fund Records[11] | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | No | | |
| **IMTKS5E** | **Building Management** | | | | | | | | | |
| IMTKS5E.1 | Title Deeds | | Permanent [12] | | | | Yes | No | | |
| IMTKS5E.2 | Plans | | Permanent<br>Retain in school whilst operational | | | | Yes | No | OFFICIAL [13] | |
| IMTKS5E.3 | Records relating to maintenance and contractors | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | No | | |
| IMTKS5E.4 | Maintenance log books | | Last entry + 10 years | | | | Yes | No | | |
| IMTKS5E.5 | Contractors' Reports | | Current year + 6 years | | | | Yes | No | | |
| IMTKS5E.6 | Leases | | Expiry of lease + 6 years | | | | Yes | No | | |
| IMTKS5E.7 | Lettings | | Current year + 3 years | | | | Yes | No | | |
| IMTKS5E.8 | Burglary, theft and vandalism report forms | | Current year + 6 years | | | | Yes | No | | |
| IMTKS5E.9 | Records relating to legionella and water checks | The Management of Health & Safety at Work Regulations 1999 Health and Safety at Work Act 1974 | Date of check + 3 years | | | | Yes | No | | |
| **IMTKS5F** | **School Meals** | | | | | | | | | |
| IMTKS5F.1 | Dinner Register | | Current year + 3 years | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS5F.2 | School Meals Summary Sheets | | Current year + 3 years | | | | No | No | | |
| IMTKS5F.3 | Free school meals registers | HMRC - Compliance Handbook Manual CH15400 | Current year + 6 years | | | | Yes | Yes | OFFICIAL | |
| **IMTKS5G** | **General Administration** | | | | | | | | | |
| IMTKS5G.1 | School brochure/prospectus | | Current year + 3 years | | | | No | No | | |
| IMTKS5G.2 | General file series or correspondence files | | Current year + 5 years | | | | No | No | | |
| IMTKS5G.3 | Circulars (staff/parents/pupils) | | Current year + 1 year | | | | No | No | | |
| IMTKS5G.4 | Newsletters, ephemera | | Current year + 1 year | | | | No | No | | |

[11] including cheque books, paying in books, ledgers, invoices, receipts, bank statements, school journey books
[12] these should follow the property unless the property has been registered at the Land Registry
[13] These records carry an OFFICIAL marking as there can be security issues about allowing access to the plans of buildings to people who may be looking to burgle the premises

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS5G.5 | Visitors book | | Current year + 2 years | | | | No | Yes | OFFICIAL | |
| IMTKS5G.6 | Images held of pupils together with any consents and permissions to publish | | All records relating to the image should be retained for the life of the image. The length of time the image is to be retained should be included on the privacy statement | | | | Yes | Yes | OFFICIAL | |
| IMTKS5G.7 | Records relating to the management of PTA/Old Pupils Associations | | Current year + 6 years | | | | No | Yes | OFFICIAL | |
| IMTKS5G.8 | Records relating to the management of data subject access requests | | Current year + 3 years | | | | No | Yes | OFFICIAL | |
| IMTKS5G.9 | Records relating to the management of freedom of information requests | | Current year + 3 years | | | | No | Yes | OFFICIAL | |

## IMTKS6 Management of Schools – Safeguarding

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS6A** | **Adults** | | | | | | | | | |
| IMTKS6A.1 | Records of allegations about workers who have been investigated and found to be without substance | Information Commissioner Code of Practice: Employment Records 2002 - "Child Protection Procedures for Managing Allegations Against Staff within Schools and Education Services" (September 2008) p17 | These records should not normally be retained once an investigation has been completed[14]. | | | | Yes | Yes | OFFICIAL SENSITIVE | |
| IMTKS6A.2 | Outcome of an allegation made against a staff member | Safeguarding Children in Education Guidelines: Dealing with Allegations of Abuse against Teachers and Other Staff Safeguarding Children in Education and Safer Recruitment 2007 Para 5.1 | Until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer | | | | Yes | Yes | OFFICIAL SENSITIVE | |

## IMTKS7 Central Government and Local Authority

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| **IMTKS7A** | **Local Authority** | | | | | | | | | |
| IMTKS7A.1 | Secondary transfer sheets (Primary) | | Current year + 2 years | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS7A.2 | Attendance returns | | Current year + 1 year | | | | No | No | | |

[14] There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example where the allegation relates to abuse and the worker is employed to work with children or other vulnerable adults

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS7A.3 | Circulars from LA | | Whilst required operationally then review to see whether a further retention period is required | | | | No | No | | |
| **IMTKS7B** | **Central Government** | | | | | | | | | |
| IMTKS7B.1 | OFSTED reports and papers | | Replace former report with any new inspection report then review to see whether a further retention period is required | | | | No | No | | |
| IMTKS7B.2 | Returns | | Current year + 6 years | | | | No | No | | |
| IMTKS7B.3 | Circulars from DfE | | Whilst operationally required then review to see whether a further retention period is required | | | | No | No | | |

## IMTKS8 Family Liaison Officers and Parent Support Assistants

| | | | | Information Asset Register Information | | | | | | Information Risk Register Information |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Basic file description** | **Statutory Provisions** | **Retention Period** | **Information Asset Owner** | **Principal Copy** | **Principal Record Keeper** | **Business Critical** | **Personal Information** | **Protective Marking** | **Information Risk Category** |
| IMTKS8.1 | Day Books | | Current year + 2 years then review | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS8.2 | Reports for outside agencies – where the report has been included on the case file created by the outside agency | | Whilst the child is attending the school then destroy | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS8.3 | Referral forms | | While the referral is current then add to child's file | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS8.4 | Contact data sheets | | Current year then review, if contact is no longer active then destroy | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS8.5 | Contact database entries | | Current year then review, if contact is no longer active then destroy | | | | No | Yes | OFFICIAL SENSITIVE | |
| IMTKS8.6 | Group Registers | | Current year + 2 years | | | | No | Yes | OFFICIAL SENSITIVE | |

Please note that the Family Liaison Officer records will not normally be shared with the head teacher without the consent of the parents. For more information please contact Michelle Hunt.

## 5.7 Disposal of Records

It is important that schools dispose of records in a way that minimises the possibility of an information security breach. For example, all records containing personal information, or sensitive policy information should be made either unreadable or disposed of in a way that they could not be reconstructed (i.e. it should not be possible to reconstruct shreds to make the document).

### 5.7.1 Recording the disposal of records

The school should keep a record of the information which has been disposed of and on whose authority they have been disposed of.

**Sample Disposal Schedule**

The following records were destroyed according to the retention period laid down in the school retention schedule or on the authorisation of the officer named below*.

*delete as appropriate

Signed:

Date:

| File Reference | Brief Description | On whose authority | Method of disposal |
|---|---|---|---|
| | | | |
| | | | |

### 5.7.2 Appropriate disposal methods

Physical records which contain personal information, sensitive policy information or commercially sensitive information should be shredded using a cross-cutting shredder. Ideally they should be shredded on the premises. This will include all records with the protective marking categories OFFICIAL and OFFICIAL SENSITIVE.

If the school does not have access to a shredder or does not have the staff resource to complete the shredding (for example, in a big Secondary School, considerable resource may be required to shred the pupil records which are no longer required) please contact the Records Manager, Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk who can advise about the use of external shredding companies and the costs attached to this.

Physical records which do not meet the criteria outlined above can be disposed of using standard disposal methods. This may include waste paper bins or recycling bins. If the school disposes of records on a routine basis (e.g. once a year) and hires a skip for the purpose then where possible the skip should have a secure lid. It is not recommended that records are disposed of in the same skip as furniture or other equipment.

If the school is unsure about which category records fall into then it is safer to treat the records as though they were OFFICIAL or OFFICIAL SENSITIVE.

CDs / DVDs / Floppy Disks should be cut into pieces or alternatively can be put through the shredder. Most shredders have an attachment which will allow for the disposal of CDs and DVDs.

Audio / video tapes and fax rolls should be dismantled and shredded. Be careful when shredding fax rolls which consist of film as these give off a toxic vapour as the film heats up on its way through the shredder.

### 5.7.3 Certificate of Destruction

If the school employs an external company to dispose of records, the company must supply the school with a certificate of destruction to document that the records have been disposed of. All the reputable companies are aware of this requirement and will usually offer a certificate of destruction as standard.

## 5.8 Business Continuity

Business continuity is an integral part of managing records under both Data Protection Act 2018/General Data Protection Regulations 2016 and the Freedom of Information Act 2000. It is also important to ensure that if a major incident does occur then individual schools can stay open and ensure that all the information which is required is available.

There are two main areas where schools may be affected by business continuity issues:

- Major computer failure (i.e. theft of computers or corruption of data)
- Environmental incidents (i.e. fire or flood)

### 5.8.1 Major Computer Failure

Major computer failure can take two forms, but in both cases, a robust back up system is vitally important.

There are two areas of concern when computers are stolen. In the first place, the data on the computers (some of it sensitive personal data) could fall into the wrong hands and be misused by the individuals who have stolen the computers. Do not store sensitive personal information on the hard drives of either desk top or lap top computers unless absolutely necessary (e.g. you are taking a lap top home to work on data). All sensitive information should be stored on network drives where possible. If the server is on the school premises, ensure that the data is subject to a robust password protection regime and that the server is stored in a place which has adequate security.

If the electronic data becomes corrupted on the server then the school will need to ensure that they can restore the regular backups.

The school should undertake regular backups of all information held electronically so that data can be installed on any new equipment which has been purchased or reinstalled once the corrupted data has been removed. Where possible these backups should be stored off the main school site. In the event of a fire backups can be destroyed or corrupted along with other data (even if they are in a safe). It is also possible that the emergency services will not allow members of staff back on the site to pick up any backups for a number of days after any incident has occurred. In the case of theft, if the safe is stolen along with the computers then the backups could be stolen along with the computers.

### 5.8.2 Major Environmental Incident

Fire and flood are two major threats to schools. These threats pose a greater risk to paper records than to electronic records (provided that the school has a robust backup procedure). In the event of a flood most if not all records can be salvaged. Fire, however, can be much more destructive of records and although fire damaged material can be salvaged it can be much harder.

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. Water damage is always much less severe if the water has first had to get into a receptacle. Metal filing cabinets have, in the past, proved a good first level barrier against fire (provided the heat does not force the drawers open).

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.

Individual schools need to undertake business risk analysis to identify which records are vital to school management and these records should be stored in a container. Reference material or material which could be easily replaced (phone books, supplies catalogues etc) can be stored on open shelves or desks.

For any further advice about business continuity issues in the record keeping context please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk.

## 5.9 Creating an Information Management Manual

Once the school has developed an information management programme, the final stage is to document all the different processes. One of the ways this can be done is by creating an information management manual using the different headings outlined in section 5.

If you would like further information about how to develop an Information Management Manual please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk

## 6. Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil wherever they find themselves in the Education system and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file cover).

It has become clear over a series of information audits that there is no real consistency of practice in the way in which pupil records are managed. These are intended to be guidelines to assist schools about how pupil records should be managed and what kind of information should be included in the file. It is hoped that the guidelines will develop further following suggestions and comments from those members of staff in schools who have to deal with these records.

These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact Michelle Hunt (Information Governance Specialist) on michelle.hunt@kent.gov.uk for advice.

### 6.1 File covers for pupil records

It is strongly recommended that schools use a consistent file cover for the pupil record. This assists the Secondary School to ensure consistency of practice when receiving records from a number of different Primary Schools and also ensures that the same level of information is held for all pupils. For example, in one Secondary School there were at least three different kinds of file cover transferred for that year's intake. This led to the Secondary School holding different levels of information for pupils which had come from different Primary Schools.

The pre-printed file covers issued by Kent County Supplies are a good example of best practice and should be used where possible. The use of standard document wallets should be avoided as it is very difficult to ensure that all the information required by the school is recorded consistently.

By using pre-printed file covers all the necessary information is collated and the record looks tidy and reflects the fact that it is the principal record containing all the information about an individual child.

### 6.2 Recording information

A pupil or their nominated representative can ask to see their file at any point during their education (and indeed until they reach the age of 25 years when the record is destroyed). It is important to remember that all information should be accurate and objective and expressed in the appropriate language.

### 6.2.1 Primary School records

### 6.2.1a Opening a file

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career. If the pre-printed file covers are not being used then the following information should appear on the front of the file:

- Surname
- Forename
- DOB
- Gender
- Position in family
- Ethnic origin [although this is "sensitive" data under the Data Protection Act 2018/General Data Protection Regulations 2016, the DfE require statistics about ethnicity]
- Language of home (if other than English)
- Religion [although this is "sensitive" data under the Data Protection Act 2018/General Data Protection Regulations 2016, the school has good reasons for collecting the information]
- Names of parents and/or guardians with home address and telephone number
- Name of the school, admission number and the date of admission and the date of leaving.

Inside the front cover the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details

There has been some discussion about whether or not the pupil's UPN should be recorded on the front of the file with the other information. It is perfectly acceptable to include the UPN on the front of the file as the computer system is password protected.

It is essential that as these files contain all this personal information that they will be managed against the information security guidelines also contained in the toolkit.

### 6.2.1b Items which should be included on the pupil record

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file
- Admission form (application form)
- Fair processing notice [if these are issued annually only the most recent need be on the file]
- Parental permission for photographs to be taken (or not)
- Kent Years Record
- Annual Written Report to Parents

- National Curriculum and R.E. Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in an envelope)
- Child protection reports/disclosures (should be stored in the file in an envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files before they are transferred on to another school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

### 6.2.1c Transferring the pupil record to the Secondary School

The pupil record should not be weeded before transfer to the Secondary School unless any of the items mentioned above have been placed on the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Primary Schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of, and therefore responsibility for, the records passes to the school the pupil transfers to.

If files are sent by post, they should be sent by registered post with an accompanying list of the files. Where possible, the Secondary School should sign a copy of the list to say that they have received the files and return that to the Primary School. Where appropriate records can be delivered by hand.

**Please note that if the pupil leaves the primary school and either joins an independent school, is home educated, moves abroad or moves to a school unknown to the primary school then the pupil file should be sent to the Information Resilience and Transparency Team, Room 2.89 Sessions House, Maidstone, for archiving. The records should be marked for the attention of Elizabeth Barber.**

### 6.2.2 Secondary School records

#### 6.2.2a Items which should be included on the pupil record

- Admission form (application form)
- Privacy notice [if these are issued annually only the most recent need be on the file]
- Parental permission for photographs to be taken (or not)
- Kent Years Record
- Annual Written Report to Parents
- National Curriculum and R.E. Agreed Syllabus Record Sheets
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in an envelope)
- Child protection reports/disclosures (should be stored in the file in an envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files once the pupil Leaves the school.

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

### 6.3 Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school Leaving age (or the school where the pupil completed sixth form studies) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by minor for up to 7 years from their 18th birthday.

### 6.4 Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact Michelle Hunt (Information Governance Specialist); michelle.hunt@kent.gov.uk for further advice.

If you have any comments about these guidelines or suggestions about how they can be further developed please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk.

## 7. School Closures and Record Keeping

When a school closes there will be records which will need to be stored until they work out their statutory retention periods. A full list of records can be found in the retention guidelines but some examples might include:

- Pupil records (DOB of pupil + 25 years)
- Accident reporting records (DOB of pupil + 25 years or date of incident + 7 years)
- Financial records (Current year + 6 years)
- Records relating to the employment of staff (Termination + 7 years)

It is the responsibility of the Local Authority to manage these records until they have reached the end of their administrative life and to arrange for their disposal when appropriate.

There may be a number of different reasons why a school has closed and this may affect where the records need to be stored.

- If the school has been closed and the site is being sold or reallocated to other use then the LA should take responsibility for the records from the date the school closes.
- If two schools have merged onto one site and then function as one school, it is sensible to retain all the records relating to the two schools on the one site.
- If a secondary school closes and subsequently becomes an Academy, the records relating to the current pupil intake will be transferred to the Academy, but all other records become the responsibility of the LA.

Sorting out records, when a building has to be vacated, is time consuming especially if records management has not been a priority in the past. Sufficient time to ensure that the records have been properly sorted, listed and boxed before transfer to the LA must be allowed as part of the project timescales for the school closure. Proper resources must be allocated to this to ensure that the job can be completed before the school closes. It is much more difficult to sort records which have been boxed haphazardly in a hurry in the few days before the school closes.

It is important to bear in mind that when a school closes the staff teams may well feel a real sense of bereavement and this will affect the way in which they view the work which has to be done before the school closes. Sorting out records is usually low on the priority list, but nonetheless needs to be tackled. Managers will need to consider this when allocating the different elements of the task.

It is suggested that a project to sort out records could be managed in the following steps:

1. As soon as notification is received that the school is to be closed, a thorough review of all the records on the premises needs to take place. Agreement needs to be reached with the LA about where the records which need to be stored until they can be disposed of will be sent and who in the LA will be taking responsibility for them.

2. At this stage, if it has been decided to transfer records to the Records Management Service, it is useful to make initial contact with the Records Management Service team on 03000 411802. This is a good opportunity to find out how the system works, order boxes and look at the allocation of RMS code numbers.

3. The next step is to identify all the records which can be safely disposed of using the retention guidelines. If you are unsure about what records can be safely disposed of contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk.

4. This should leave you with a list of the records which need to be transferred to the LA. If it has been decided to send records to the RMS then e-mail a list of the record series (e.g. pupil files, accident reports etc) to the RMS team and they will allocate RMS reference numbers for you to use.

5. The records need to be boxed up and listed in accordance with RMS procedures and sent to the RMS at Kings Hill.

If records need to be recalled to answer enquiries, this will be done by the LA.

If you need further advice or assistance about how to manage records for a closed school please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk or Michelle Hunt (Information Governance Specialist); michelle.hunt@kent.gov.uk .

## 8. Digital Continuity

The long term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise.

In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 7 years should be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 7

years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

## 8.1 The Purpose of Digital Continuity Statements

A digital continuity statement will not need to be applied to all the records created by the school. The retention schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 7 years needs to be subject to a digital continuity statement.

Appropriate records need to be identified as early in their lifecycle as possible so that the relevant standards can be applied to them and conversely any records which do not need to be included in the policy should also be identified in the early part of the lifecycle. Digital continuity statements should only be applied to principal copy records.

## 8.2 Allocation of Resources

Responsibility for the management of the digital continuity strategy, including the completion of the digital continuity statements should rest with one named post holder. This will ensure that each information assets is “vetted” for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

## 8.3 Storage of records

Where possible records subject to a digital continuity statement should be “archived” to dedicated server space which is being backed up regularly.

Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen.

Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy.

## 8.4 Migration of Electronic Data

Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible system specifications should state the accepted file formats for the storage of records within the system.

If data migration facilities are not included as part of the specification, then the

system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project.

Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

## 8.5 Degradation of Electronic Documents

In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable.

When electronic records are transferred from the main system to an external storage device, the data should be backed up and two safe copies of the data should be made. The data on the original device and the back-ups should be checked periodically to ensure that it is still accessible. Additional back-ups of the data should be made at least once a year and more frequently if appropriate.

Where possible digital records should be archived within a current system, for example, a designated server where “archived” material is stored or designated storage areas within collaborative working tools such as SharePoint.

## 8.6 Internationally Recognised File Formats

Records which are the subject of a digital continuity statement must be “archived” in one of the internationally recognised file formats. For further information about these file formats please contact Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk .

## 8.7 Exemplar Digital Continuity Strategy Statement

An exemplar digital continuity strategy statement can be found at Appendix C.

## 8.8 Review of Digital Continuity Policy

The Digital Continuity Policy should be reviewed on a bi-annual (or more frequently if required) basis to ensure that the policy keeps pace with the development in technology.

# 9. Information Security

Information security is an integral part of the Data Protection Act 2018/General Data Protection Regulations 2016. You must take all reasonable steps to ensure that any personal or sensitive information which the school is collecting and storing is securely stored.

## 9.1 Personal Data Breach

The Information Commissioner can now fine organisations €20 million or 4% of annual turnover of the previous year, whichever is higher for serious personal data breaches and the number of fines is increasing.

If, despite the security measures you take to protect the personal data the school holds, a breach of security occurs, it is important to deal with the breach effectively. The breach may arise from a theft, a deliberate attack on computer systems (for example, someone has managed to "hack" the system), the unauthorised use of personal data by a member of staff, accidental loss or equipment failure.

## 9.2 Reporting a Personal Data Breach

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it.

**You do not need to report every breach to the ICO.**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. **You must do this within 72 hours of becoming aware of the breach**, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the ICO and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Failing to notify a breach when required to do so can result in a significant fine of up to 10 million euros or 2 % of your annual turnover. The fine can be combined with the ICO's other corrective powers under Article 58 of the GDPR. Therefore it's important

to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

For more information about what a personal data breach is and when you need to report it to the ICO, please follow this link to the ICO website: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

If you would like advice about whether to report an incident to the Information Commissioner's Office, please contact Michelle Hunt (Information Governance Specialist); michelle.hunt@kent.gov.uk .

### 9.3 Information Security Guidelines

You will find below some guidelines to bear in mind when considering information security:

1. All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended. Personal information should not be left on your desk where anyone could see it. You might need to consider restricting access to offices in which personal information is being worked on or stored.

2. If you are "archiving" information somewhere else in your own building (or in an outbuilding) make sure that the door can be locked and that the key is kept locked away. Anyone accessing the room should sign for the key. Where possible, there should be a file tracking system where anyone borrowing items from the "archive" room must make a note of what they have taken.

3. Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended. Make sure that you don't have shared passwords to systems (or share personal passwords with other members of staff) and that all members of staff log off the computer when it is left unattended.

4. Ensure that your computer screen cannot be viewed by an unauthorised person.

5. If you have a laptop or any electronic mobile device which holds personal data, make sure it is encrypted.

6. Do not send personal information by unsecured email as its security cannot be guaranteed. If it is necessary to send information in this way and you do not have access to secure email, make sure the personal information has been either password protected or de-personalised. Send the data as an attachment to the email and flag as confidential.

7. If sending any email to multiple recipients outside of the school, consider using blind copy facility (bcc) so recipients can't view other recipients' email addresses.

8. If records need to be taken off the school premises they should be secured in a lockable box or briefcase and put in the boot of the car. Any records or devices containing personal information (e.g. laptops, PDAs, briefcases etc) should not be

left unattended for any length of time especially in a car overnight. Once you have removed the records from the car and secured them in your home, make sure that they are not left out for general access to other family members in your home.

9. If using a home computer (or laptop) to process personal information ensure you have up-to-date virus protection software installed. No other members of your household should have access to the computer or the information contained on it. Any documents produced should be stored onto disk and not to the hard drive.

10. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the caller's name and switchboard telephone number and verify their details before responding.

11. Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.

One of the best rules of thumb for dealing with sensitive, personal information, is to ask the question "if this was my information would I be happy with the way in which it is being treated?"

The best ways of disposing of sensitive, personal information are dealt with in section 5.7 which looks at 'disposal of records'.

For more information on Information Security, please see the relevant pages on KELSI at this link: http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/information-security

If you need to know any more about information security please contact either Michelle Hunt (Information Governance Specialist); michelle.hunt@kent.gov.uk or Elizabeth Barber (Records Manager); elizabeth.barber@kent.gov.uk .

## Appendix A Model Records Management Policy[15]

**X School - Records Management Policy**

The School recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. This document provides the policy framework through which this effective management can be achieved and audited. It covers scope, responsibilities and relationships with existing policies.

**1. Scope of the policy**

1.1 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research.

**2. Responsibilities**

2.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

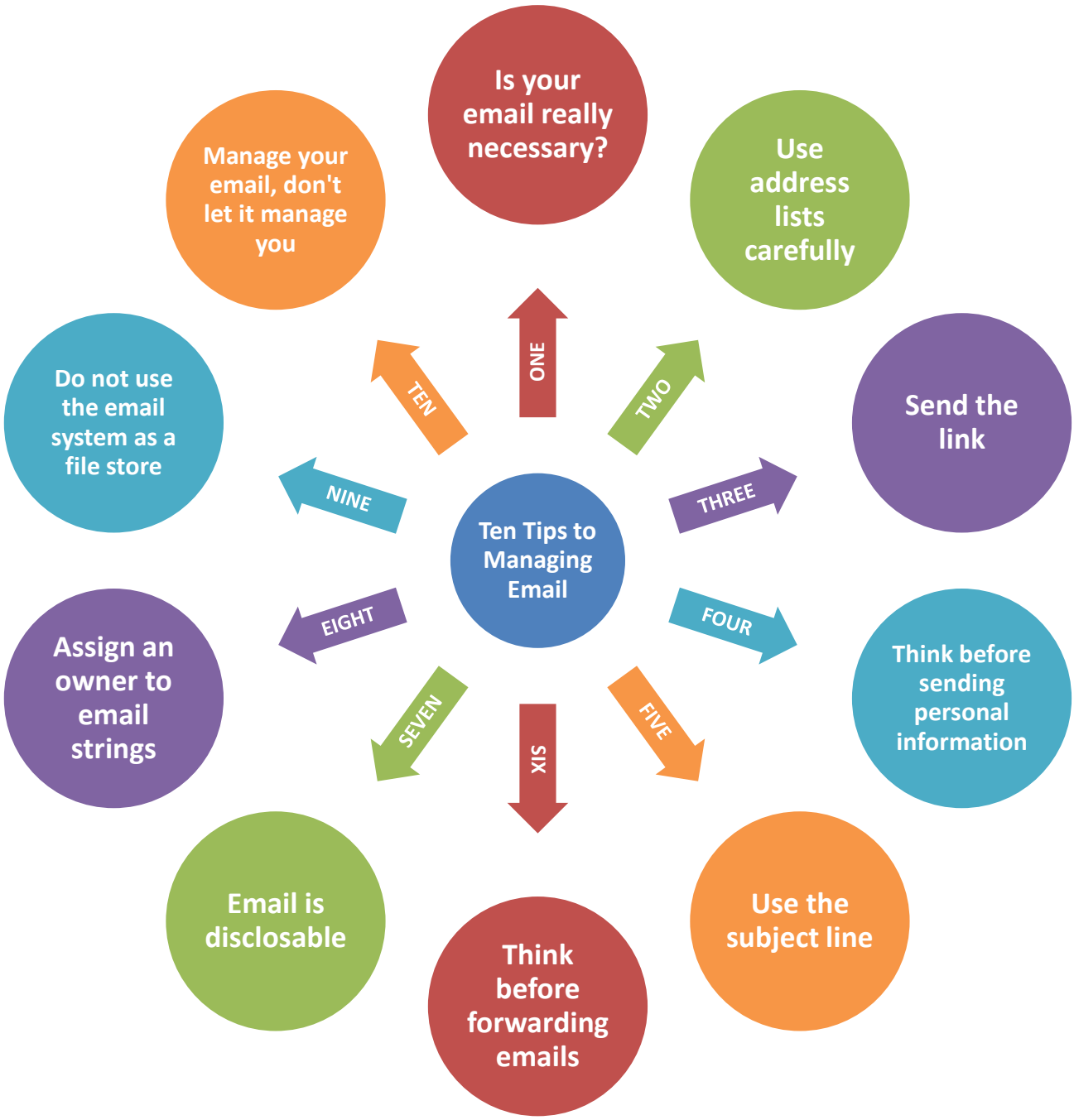
2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

**3 Relationship with existing policies**

This policy has been drawn up within the context of: Freedom of Information policy, Data Protection policy and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

[15] Extracted from Model action plan for developing records management compliant with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000 Model Action Plan for Schools (Appendix A). [To see the full action plan see www.nationalarchives.gov.uk/documents/schools.rtf]

## Appendix B Ten Tips to Help Manage Email




**1 Is your email really necessary?**

Ask the question, “does this transaction need to be done by email. It may be more appropriate to use the telephone or to speak face to face.

**2 Use address lists carefully**

Ensure that you have addressed the email to the correct person and avoid the use of address list groups. Also bear in mind that if all the addresses are

visible that this could constitute a breach under the Data Protection Act 2018/General Data Protection Regulations 2016.

Check your address groups regularly to ensure that only the correct recipients are a part of the group.

**3 Send the link**

Email has been used traditionally for transporting information electronically. This can lead to large files being sent to a big group of people which then clogs up the email system. If possible put documents in a central place and send the link to individuals rather than sending the document itself.

**4 Think before sending personal/confidential information via email**

Email which is sent via the web can be routed via a number of different ISPs, which may be hosted in a number of different countries. Even on the secure internal email system email can be mis-sent.

You need to think about information security issues when you decide to send confidential information by email. The consequences of an email containing sensitive information being sent to an unauthorised person could be a fine from the Information Commissioner. Other information, if mis-sent, could end up on the front page of a newspaper.

Where possible personal information should not be transported using the email system unless the sender and the recipient both have secure email accounts or are using encryption techniques.

If there is no other alternative the following criteria should be observed.

- Do not include information that will identify the individual in the subject line (for example, name, date of birth, UPN or other identifier).
- Do not include personal information in the body of the email.
- Make sure that the personal information is contained in a separate document which should be password protected where appropriate and attached to the email.
- Make sure that you send the password in a separate email or telephone the recipient to give them the password.
- Include some text in the body of the email informing recipients what they should do if they have received the email in error.

**5 Use the subject line**

Having a clearly defined subject line assists the recipient to sort the email on receipt. A clear subject line also assists in filing all emails relating to individual projects together. For example, the subject line might be the name of the policy, or the file reference number.

**6 Think before forwarding emails**

Before forwarding emails onto other members staff, make sure that you have the permission of the sender to forward the information. The information may be copyright to someone other than KCC or the intellectual property rights may belong to someone else.

## 7 Email is disclosable and can form part of a legal process

As email is used for all types of correspondence there is the danger that people phrase emails more informally than they would other documents such as memos. All email is disclosable under Freedom of Information and Data Protection legislation.

There is a tendency to phrase email in a more informal way than standard correspondence. This can cause issues where the email becomes disclosable under the Data Protection Act 2018/General Data Protection Regulations 2016 or the Freedom of Information Act 2000. Information within an email cannot be redacted simply because it will cause embarrassment to the school when it is disclosed.

Agreements entered into by email do form a contract. Members of staff need to be aware of this if they enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of KCC or with external contractors unless they are authorised to do so.

The courts have held that agreements, however informally expressed in email are still legally binding and may be treated in the same way as a more formal contract. Therefore, email should be phrased in the same way that a more formal method of communication would be.

## 8 Assign an owner to email strings

Each email string which constitutes a principal record should be allocated a principal record keeper who will be responsible for ensuring that one copy of the email string is retained as the record of the conversation and that all unnecessary duplication is removed. All discussion which does not directly relate to the final outcome should be removed. Where there are several strings to the same email (i.e. two people replied to the email simultaneously) then each string should be treated as an individual record. (see section 9.2 above)

## 9 Do not use the email system as a file store

The email system is intended to be a vehicle for transporting information. The email system should not be used as a storage system.

Email should be transferred to the appropriate electronic folder in .msg format. However, other options include transfer in .html, .rtf or .txt format using the “save as” facility. This is not advised as metadata hidden in the .msg format is

lost[16]. This format will also not support the attachment (i.e. the attachment will be lost).

Alternatively, email can also be printed to or saved as pdf format. This is not advised for the same metadata reasons above unless the information in the email is being treated in the same way as physical correspondence would be. Email can also be printed on to paper. This is not advised for the same metadata reasons above unless the information in the email is being treated in the same way as physical correspondence would be or unless the service unit is managing a predominantly paper based system.

## 10 Manage your email, don't let it manage you

Remember that although email may be important, it is not always urgent. Email may not always require an instant response. There are workflow techniques which are available to assist you manage the email.

[16] This can cause an issue in proving legal admissibility should the email be required in a future legal case.

## Appendix C Exemplar Digital Continuity Strategy Statement

Each digital continuity statement should include the following information:

1. **Statement of business purpose and statutory requirements for keeping records**

   **The statement should contain a description of the business purpose for the information assets and any statutory requirements including the retention period for the records. This should also include a brief description of the consequences of any loss of data.**

   By doing this the records owner will be able to show why and for how long the information assets needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets which require them.

2. **Names of the people/functions responsible for long term data preservation**

   **The statement should name the post-holder who holds responsibility for long term data preservation and the post holder responsible for the information assets. The statement should be updated whenever there is a restructure which changes where the responsibility for long term data preservation is held.**

   If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

3. **Description of the information assets to be covered by the digital preservation statement**

   **A brief description of the information asset taken from the IAR.**

4. **Description of when the record needs to be captured into the approved file formats**

   **The record may not need to be captured in to the approved file format at its creation. For example, an MSWord document need not be converted to portable document format until it becomes semi-current. The digital preservation statement should identify when the electronic record needs to be converted to the long term supported file formats identified above.**

   Workflow process diagrams can help identify the appropriate places for capture.

5. **Description of the appropriate supported file formats for long term preservation**

   This should be agreed with the appropriate technical staff.

6. **Retention of all software specification information and licence information**

   **Where it is not possible for the data created by a bespoke computer system to be converted to the supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety.**

   If this information is not retained it is possible that the data contained within the system may become inaccessible with the result that the data is unusable with all the ensuing consequences

7. **Description of where the information asset is to be stored.**

   See section 4 above.

8. **Description of how access to the information asset is to be managed within the data security protocols**

   **The data held for long term preservation must be accessible when required but also must be protected against the standard information security requirements which are laid down for records within the authority. The statement must contain the policy for accessing the records and the information security requirements attached to the information assets.**

| **Useful Contacts** | | | |
|---|---|---|---|
| Elizabeth Barber | Records Manager | 03000 415812 | Elizabeth.barber@kent.gov.uk |
| Michelle Hunt | Information Governance Specialist | 03000 416286 | Michelle.hunt@kent.gov.uk |
| Sarah Stanley | Service Development Manager – Heritage | 03000414943 | Sarah.stanley@kent.gov.uk |