Retention of Records Template

Chatham & Clarendon Grammar School

May 2018

1 Recommended Retention Periods

CCGS1 Governors

				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**	**Protective Marking**	**Information Risk Category**
CCGS1.1	Minutes - Principal set (signed)		Permanent				YES	PROTECTED	
CCGS1.2	Minutes - Inspection copies		Date of meeting + 3 years				NO	OPEN	
CCGS1.3	Agendas – Principal copy		Permanent				YES	OPEN	
CCGS1.4	Agendas – Additional Copies		Date of meeting				NO	OPEN	
CCGS1.5	Reports		Date of report + 7 years				YES	PROTECTED	
CCGS1.6	Annual Parents' meeting papers		Date of meeting + 7 years				YES	OPEN	
CCGS1.7	Instruments of Government		Permanent				YES	OPEN	
CCGS1.8	Trusts and Endowments		Permanent				YES	OPEN	
CCGS1.9	Action Plans		Date of action plan + 3 years				YES	OPEN	
CCGS1.10	Policy documents		Expiry of policy Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)				YES	OPEN	
CCGS1.11	Complaints files		Date of resolution of complaint + 6 years then review for further retention in the case of contentious disputes				YES	RESTRICTED	
CCGS1.12	Annual Reports required by the Department for Education	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI	Date of report + 10 years				YES	OPEN	
CCGS1.13	Proposals for schools to become, or be established as Specialist Status schools		Current year + 3 years				YES	OPEN	

CCGS2 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**	**Protective Marking**	**Information Risk Category**
CCGS2.1	Log Books		Date of last entry in the book + 6 years				Yes	OPEN	
CCGS2.2	Minutes of the Senior Management Team and other internal administrative bodies		Date of meeting + 5 years				Yes	PROTECTED	
CCGS2.3	Reports made by the head teacher or the management team		Date of report + 3 years				Yes	PROTECTED	
CCGS2.4	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	PROTECTED	
CCGS2.5	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	PROTECTED	
CCGS2.6	Professional development plans		Closure + 6 years				Yes	OPEN	
CCGS2.7	School development plans		Closure + 6 years then review				Yes	OPEN	
CCGS2.8	Admissions – if the admission is successful		Admission + 1 year				Yes	RESTRICTED	
CCGS2.9	Admissions – if the appeal is unsuccessful		Resolution of case + 1 year				Yes	RESTRICTED	
CCGS2.10	Admissions – Secondary Schools – Casual		Current year + 1 year				Yes	RESTRICTED	
CCGS2.11	Proofs of address supplied by parents as part of the admissions process		Current year + 1 year				Yes	RESTRICTED	

CCGS3 Pupils

				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**	**Protective Marking**	**Information Risk Category**
CCGS3.1	Admission Registers		Permanent				Yes	RESTRICTED	
CCGS3.2	Attendance registers		Date of register + 3 years				Yes	RESTRICTED	
CCGS3.3	Pupil record cards - Primary		Retain for the time which the pupil remains at the primary school Transfer to the secondary school (or other primary school) when the child leaves the school[1]				Yes	RESTRICTED	
CCGS3.4	Pupil record cards - Secondary		Permanent				Yes	RESTRICTED	
CCGS3.5	Pupil Files - Primary		Retain for the time which the pupil remains at the primary school Transfer to the secondary school (or other primary school) when the child leaves the school[1]				Yes	RESTRICTED	
CCGS3.6	Pupil Files - Secondary		DOB of the pupil + 25 years[1]				Yes	RESTRICTED	
CCGS3.7	Special Educational Needs files, reviews and Individual Education Plans		DOB of the pupil + 25 year[1]				Yes	RESTRICTED	
CCGS3.8	Letters authorising absence		Date of absence + 2 years				Yes	RESTRICTED	
CCGS3.9	Absence books		Current year + 6 years				Yes	RESTRICTED	
CCGS3.10	Examination results - Public		Year of examinations + 6 years[2]				No	OPEN	
CCGS3.11	Examination results - Internal examination results		Current year + 5 years 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	OPEN	
CCGS3.12	Any other records created in the course of contact with pupils		Current year + 3 years then review				Yes	RESTRICTED	
CCGS3.13	Statement maintained under The Education Act 1996 - Section 324	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years Unless legal action is pending				Yes	RESTRICTED	

[1] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service
[2] 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**	**Protective Marking**	**Information Risk Category**
CCGS3.14	Proposed statement or amended statement	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years Unless legal action is pending				Yes	RESTRICTED	
CCGS3.15	Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years Unless legal action is pending				No	RESTRICTED	
CCGS3.16	Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years Unless legal action is pending				Yes	RESTRICTED	
CCGS3.17	Pupil SEN Files		DOB of pupil + 30 years then review – it may be appropriate to add an additional retention period in certain cases Unless legal action is pending				Yes	RESTRICTED	
CCGS3.18	Parental permission slips for school trips – where there has been no major incident		Conclusion of the trip				Yes	RESTRICTED	
CCGS3.19	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 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	RESTRICTED	
CCGS3.20	Primary 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 + 14 years[4]				Yes	RESTRICTED	
CCGS3.21	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	RESTRICTED	
CCGS3.22	Walking Bus registers		Date of register + 3 years [5]				Yes	RESTRICTED	

[3] including GOF1 and GOF2 and data entered on the e-go system
[4] This retention period has been set in agreement with the Safeguarding Children's Officer
[5] 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

CCGS 4Curriculum

				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**	**Protective Marking**	**Information Risk Category**
CCGS4.1	Curriculum development		Current year + 6 years				No	OPEN	
CCGS4.2	Curriculum returns		Current year + 3 years				No	OPEN	
CCGS4.3	School syllabus		Current year then review				No	OPEN	
CCGS4.4	Schemes of work		Current year then review				No	OPEN	
CCGS4.5	Timetable		Current year then review				No	OPEN	
CCGS4.6	Class record books		Current year then review				No	OPEN	
CCGS4.7	Mark Books		Current year then review				No	OPEN	
CCGS4.8	Record of homework set		Current year then review				No	OPEN	
CCGS4.9	Pupils' work		Current year then review				No	OPEN	
CCGS4.10	SATS records including examination results. Exam papers should only be retained if they are required to evidence the results		Current year + 6 years				Yes	RESTRICTED	

CCGS5 Personnel Records Held in School

				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**	**Protective Marking**	**Information Risk Category**
CCGS5.1	Timesheets, sick pay	Financial Regulations	Current year + 6 years				Yes	RESTRICTED	
CCGS5.2	Staff Personal files		Termination + 7 years[6]				Yes	RESTRICTED	
CCGS5.3	Interview notes and recruitment records		Date of interview + 6 months				Yes	RESTRICTED	

[6] These files should be subject to KCC's open file policy where the employees are employed by Kent County Council as the 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**	**Protective Marking**	**Information Risk Category**
CCGS5.4	Pre-employment vetting information (including CRB checks)	CRB guidelines	Date of check + 6 months				Yes	RESTRICTED	
CCGS5.5	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	RESTRICTED	
CCGS5.6	Disciplinary proceedings: written warning – level two		Date of warning + 12 months [7]				Yes	RESTRICTED	
CCGS5.7	Disciplinary proceedings: written warning – level one		Date of warning + 6 months[7]				Yes	RESTRICTED	
CCGS5.8	Disciplinary proceedings: oral warning		Date of warning + 6 months[7]				Yes	RESTRICTED	
CCGS5.9	Disciplinary proceedings: final warning		Date of warning + 18 months[7]				Yes	RESTRICTED	
CCGS5.10	Records relating to accident/injury at work		Date of incident + 12 years [8]				Yes	RESTRICTED	
CCGS5.11	Annual appraisal or assessment records		Current year + 5 years				Yes	RESTRICTED	
CCGS5.12	Salary cards		Permanent				Yes	RESTRICTED	
CCGS5.13	Maternity pay records	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3yrs				Yes	RESTRICTED	
CCGS5.14	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995		Current year + 6 years				Yes	RESTRICTED	
CCGS5.15	Proofs of identity collected as part of the process of checking “portable” enhanced CRB 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	RESTRICTED	

[7] If this is placed on a personal file it must be weeded from the file
[8] 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**	**Protective Marking**	**Information Risk Category**
CCGS5.16	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[9].				Yes	RESTRICTED	
CCGS5.17	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 is that is longer				Yes	RESTRICTED	

CCGS6 Health and Safety

				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**	**Protective Marking**	**Information Risk Category**
CCGS6.1	Accessibility Plans	Disability Discrimination Act	Current year + 6 years				Yes	RESTRICTED	
CCGS6.2	Accident Reporting – Students	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of birth + 25 years where the injured person is a minor at the time of the accident				Yes	RESTRICTED	
CCGS6.3	Accident Reporting – Adults	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of the accident + 4 years where the injured person is an adult at the time of the accident;				Yes	RESTRICTED	
CCGS6.4	COSHH Risk Assessments		Date of creation + 40 years				Yes	OPEN	

[9] 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**	**Protective Marking**	**Information Risk Category**
CCGS6.5	Incident reports		Current year + 20 years				Yes	RESTRICTED	
CCGS6.6	Policy Statements		Date of expiry + 1 year				Yes	OPEN	
CCGS6.7	Risk Assessments		Current year + 3 years				Yes	OPEN	
CCGS6.8	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos		Last action + 40 years				Yes	OPEN	
CCGS6.9	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation		Last action + 50 years				Yes	OPEN	
CCGS6.10	Fire Precautions log books		Current year + 6 years				Yes	OPEN	

CCGS7 Administrative

				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**	**Protective Marking**	**Information Risk Category**
CCGS7.1	Employer's Liability certificate		Closure of the school + 40 year				Yes	OPEN	
CCGS7.2	Inventories of equipment and furniture		Current year + 6 years				No	OPEN	
CCGS7.3	School brochure/prospectus		Current year + 3 years				No	OPEN	
CCGS7.4	General file series		Current year + 5 years				No	OPEN	
CCGS7.5	Circulars (staff/parents/pupils)		Current year + 1 year				No	OPEN	
CCGS7.6	Newsletters, ephemera, old school records, school magazines, school artefacts		Permanent				No	OPEN	
CCGS7.7	Visitors book		Current year + 2 years				No	OPEN	
CCGS7.8	PTA/Old Pupils Associations		Current year + 6 years				No	OPEN	

CCGS8 Financial Records Held in Schools

				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**	**Protective Marking**	**Information Risk Category**
CCGS8.1	Annual Accounts	Financial Regulations	Current year + 6 years				Yes	OPEN	
CCGS8.2	Loans and grants	Financial Regulations	Date of last payment on loan + 12 years then review to see whether a further retention period is required				Yes	OPEN	
CCGS8.3	Contracts - under seal		Contract completion date + 12 years				Yes	OPEN	
CCGS8.4	Contracts - under signature		Contract completion date + 6 years				Yes	OPEN	
CCGS8.5	Contracts - monitoring records		Current year + 2 years				Yes	OPEN	
CCGS8.6	Copy orders		Current year + 2 years				No	OPEN	
CCGS8.7	Budget reports, budget monitoring etc		Current year + 3 years				Yes	OPEN	
CCGS8.8	Invoice, receipts and other records covered by the Financial Regulations	Financial Regulations	Current year + 6 years				Yes	OPEN	
CCGS8.9	Annual Budget and background papers		Current year + 6 years				Yes	OPEN	
CCGS8.10	Order books and requisitions		Current year + 6 years				Yes	OPEN	
CCGS8.11	Delivery Documentation		Current year + 6 years				Yes	OPEN	
CCGS8.12	Debtors' Records	Limitation Act 1980	Current year + 6 years				Yes	OPEN	
CCGS8.13	School Fund Records[10]		Current year + 6 years				Yes	OPEN	
CCGS8.14	Applications for free school meals, travel, uniforms etc		Whilst child at school				No	OPEN	
CCGS8.15	Student grant applications		Current year + 3 years				Yes	OPEN	
CCGS8.16	Free school meals registers	Financial Regulations	Current year + 6 years				Yes	OPEN	
CCGS8.17	Petty cash books	Financial Regulations	Current year + 6 years				Yes	OPEN	

[10] including cheque books, paying in books, ledgers, invoices, receipts, bank statements, school journey books

CCGS9 Property Records Held in School

				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**	**Protective Marking**	**Information Risk Category**
CCGS9.1	Title Deeds		Permanent				Yes	OPEN	
CCGS9.2	Plans		Permanent Retain in school whilst operational				Yes	PROTECTED[12]	
CCGS9.3	Maintenance and contractors	Financial Regulations	Current year + 6 years				Yes	OPEN	
CCGS9.4	Leases		Expiry of lease + 6 years				Yes	OPEN	
CCGS9.5	Lettings		Current year + 3 years				Yes	OPEN	
CCGS9.6	Burglary, theft and vandalism report forms		Current year + 6 years				Yes	OPEN	
CCGS9.7	Maintenance log books		Last entry + 10 years				Yes	OPEN	
CCGS9.8	Contractors' Reports		Current year + 6 years				Yes	OPEN	

CCGS10 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**	**Protective Marking**	**Information Risk Category**
CCGS10.1	Secondary transfer sheets (Primary)		Current year + 2 years				No	RESTRICTED	
CCGS10.2	Attendance returns		Current year + 1 year				No	OPEN	
CCGS10.3	Circulars from LA		Whilst required operationally then review to see whether a further retention period is required				No	OPEN	

[12] These records carry a PROTECTED marking as there can be security issues

CCGS11 DfE

				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**	**Protective Marking**	**Information Risk Category**
CCGS11.1	OFSTED reports and papers		Replace former report with any new inspection report then review to see whether a further retention period is required				No	OPEN	
CCGS11.2	Returns		Current year + 6 years				No	OPEN	
CCGS11.3	Circulars from DfE		Whilst operationally required then review to see whether a further retention period is required				No	OPEN	

CCGS12 Connexions

				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**	**Protective Marking**	**Information Risk Category**
CCGS12.1	Service level agreements		Until superseded				Yes	OPEN	
CCGS12.2	Work Experience agreement		DOB of child + 18 years				Yes	RESTRICTED	

CCGS13 School Meals

				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**	**Protective Marking**	**Information Risk Category**
CCGS13.1	Dinner Register		Current year + 3 years				Yes	RESTRICTED	
CCGS13.2	School Meals Summary Sheets		Current year + 3 years				No	OPEN	

CCGS14 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**	**Protective Marking**	**Information Risk Category**
CCGS14.1	Day Books		Current year + 2 years then review				No	RESTRICTED	
CCGS14.2	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	RESTRICTED	
CCGS14.3	Referral forms		While the referral is current then				No	RESTRICTED	
CCGS14.4	Contact data sheets		Current year then review, if contact is no longer active then destroy				No	RESTRICTED	
CCGS14.5	Contact database entries		Current year then review, if contact is no longer active then destroy				No	RESTRICTED	
CCGS14.6	Group Registers		Current year + 2 years				No	RESTRICTED	

2. Disposal of Records

It is important that we 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 unreconstructable (i.e. it should not be possible to reconstruct shreds to make the document.)

2.1 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

2.2 Appropriate disposal methods

Physical records which contain personal information or sensitive policy information or commercially sensitive 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 PROTECTED and RESTRICTED.

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 Business Manager 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 PROTECTED or RESTRICTED.

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. Take care 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.

2.2.1 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.

2.3 Business Continuity

Business continuity is an integral part of managing records under both Data Protection Act 1998 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)

2.3.1 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.

2.3.2 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 completed destroyed in the event of fire and will be serious 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 receptacle. Reference material, or material which could be easily replaced (phone books, supplies catalogues etc) can be stored on open shelves or desks.

3. 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.

3.1 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. 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.

3.2 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.

3.2.1 Primary School records

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 1998, the DfE require statistics about ethnicity]
- Language of home (if other than English)
- Religion [although this is “sensitive” data under the Data Protection Act 1998, 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.

6.2.1 Secondary School records

6.2.2 a Items which should be included on the pupil record

- 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 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, michelle.hunt@kent.gov.uk for further advice.

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 when required 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 related 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 (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.

1. If files need to be taken off the premises they should be secured in a lockable box or briefcase and put in the boot of the car. Any items containing personal information (e.g. laptops, PDAs, briefcases etc) should not be left in a car on open view. Lap tops and data sticks should be encrypted. Physical records should not be left in the boot of a car overnight or for any extended period of time. Once you have taken the records from the car please make sure that they are not left on general access in your home. Put them out of sight in a secure environment.

2. 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.

3. 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 callers name and switchboard telephone number and verify their details before responding.

4. 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 the section 5.7 looking at the disposal of records.

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

Appendix A

Chatham & Clarendon Grammar 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 Headteacher.

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 affecting the school.

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 1998.

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 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 they 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 1998 or the Freedom of Information Act 2000. Information within an email can not 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[14]. 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 or 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 bases 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.

[14] 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.