AMDG

STONYHURST

2020-21 Academic Year

DATA PROTECTION POLICY

Name of Policy:	**Cross Campus Data Protection Policy**
Date of Policy Review:	October 2020
Revised by:	Bursar and Clerk to the Governors
Approval Body: Date Approved:	The Executive Team November 2020
Date of next revision and by whom	July 2021 – Bursar and Clerk to the Governors
Location(s) where Policy can be found	ISI Portal Stonyhurst Website Intranet Z Drive Hard copies in the following rooms: ❖ Compliance & Legal Support ❖ Headmaster's PA ❖ SMH Headmaster's PA ❖ Bursar's PA

LDS

Introduction

Stonyhurst collects, uses, creates, stores and shares large amounts of personal data on a daily basis. All members of staff whose role involves processing or creating this personal data, be it data relating to staff, pupils, parents, contractors, alumni, association members or Sports Centre members (or anyone else whose personal information we use), must be aware of our legal obligations to protect that personal data from unauthorised loss, theft or disclosure, and to process it in accordance with the law.

To ensure that we are compliant with data protection legislation we must ensure that:

- All information held by us is justifiable, by reference to its purpose;
- We are transparent and accountable as to what we hold and why we hold it;
- Personal data is held securely and accessed only by those with a legitimate reason to view it;
- We are able to respond quickly to subject access requests;
- We are able to amend, delete or transfer data promptly upon any justified request;
- Personal data collected should be auditable as far as possible;

Other Relevant Policies

Staff should be aware of other internal policies which have a bearing on the way we collect, store, and share personal data, including:

- ICT Acceptable Use Policy
- Bring Your Own Device Policy
- Taking, Storing and Using Images of Pupils Policy
- CCTV Policy
- Staff Social Media Policy

Responsibility

The Governing Body have overall responsibility for overseeing data protection compliance within Stonyhurst, and have delegated day to day responsibility for operating this policy to the Bursar, who is the Privacy and Compliance Officer for Data Protection, and he is assisted in this role by Stonyhurst's Legal Adviser.

All members of staff who process personal data on behalf of Stonyhurst have an individual responsibility to ensure that they do so in line with relevant cross-campus and departmental policies.

Review

This policy will be reviewed annually by the Bursar, with the assistance of the Legal Adviser, to ensure that the policy operates effectively and in compliance with current legislation.

Suggestions on how this policy could be improved are welcome, and should be referred to the Legal Adviser for consideration.

Protecting Personal Data at Stonyhurst

What is 'Personal Data'?

Personal Data includes everything from which a 'Data Subject' (any living individual whose data we process) can be identified. It ranges from simple contact details through to pupils' files and safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's

intentions towards an individual, and communications (such as emails) with or about them. It also includes photographs and CCTV footage (where an individual is identifiable).

Some categories of Personal Data are defined as 'special category data'. These comprise data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health or sexuality; and biometric data used for identification purposes (such as finger print records). Extra protection is afforded to special category data and we need to be particularly careful to make sure that this data is kept secure and is accessed only on a 'need to know' basis. We will usually need specific consent from individuals to process special category data (or their parents, where the individuals are pupils), and this type of data should generally not be shared outside of Stonyhurst, unless we have specific permission to do so, or where it is necessary to protect someone's vital interests (e.g. in the case of providing appropriate medical care).

Data Management

Much of appropriate data management relies on the judgement of those processing and sharing information, and for that reason this policy cannot be, and does not aim to be, completely prescriptive about the processes which individual departments, and members of staff, put in place to deal with personal data. A good starting point for making decisions about data management is to ask 'how would I want my/my child's information to be used and who would I want to be able to see it?' If you are unsure about the data management/sharing processes in your department, speak to your line manager. Line managers are encouraged to speak with the Bursar and/or the Legal Adviser if they have any concerns or questions.

Whilst 'special category data' will always be classed as being highly sensitive personal data, not all types of personal data need to be treated in the same way. In determining how much protection personal data should be given, thought should be given to how intrusive, personal or potentially embarrassing information is, and consideration should also be given to how someone might reasonably expect their personal data to be used. For example, a staff member's name, email address and training records are all 'personal data', but most staff members would not be concerned if this information was widely known or shared. They would, however, reasonably expect information relating to their disciplinary records or salary to be kept restricted to only a very few members of staff, on a need-to-know basis. Even the same type of data may need to be handled differently depending on what it records, for example, a pupil's excellent behaviour record may be disclosed more widely (including in a school assembly etc) than a pupil's poor behaviour record.

The grid below aims to give you some general guidance about the sensitivity profile of personal information. Note that special category data may include information which you may not think is obviously highly sensitive, such as religious beliefs, so any data relating to a child's Baptism, Confirmation, First Holy Communion or inclusion on a Sacramental Programme needs to be treated very carefully, as do any photographs or videos taken on behalf of Stonyhurst during or following such ceremonies. Photos and videos taken by family members are exempt from data protection law under the domestic purposes exemption.

The examples given below are for general guidance only, you should always use your professional judgement taking into account all the circumstances. The personal data of high profile parents (or pupils), or children at risk of abduction (if this has been highlighted as a concern), will need greater protection

Data Sensitivity Profile	Examples (this is not intended to be an exhaustive list)
Low	PUPILS: Names, email addresses, information about which year groups, tutor groups, playrooms, lessons and extra-curricular activities a pupil belongs to/attends, general information about trips which they are going on. Attendance records (although information about **reasons** for absence may be special category data). Group photos without names attached. PARENTS: Names and relation to child, email address CONTRACTORS: Names and contact details STAFF: Names and email addresses (including personal email addresses), work telephone numbers (direct dial and extensions), work mobile phone numbers, information about role in organisation, internal training records, job description. General attendance or punctuality records (although information about **reasons** for absence may be special category data). Correspondence (including email correspondence about work matters). GOVERNORS: Names and email addresses
Medium	EVERYONE: Next of kin details, home addresses, personal telephone numbers, Dates of Birth PARENTS: information relating to fee payment history, parental responsibility information, general information about personal circumstances (where not deemed to be highly sensitive) STAFF: appraisal review documentation, general terms and conditions, including hours worked and general benefit entitlement (although not salary), general correspondence between staff members and management about role (where not highly personal). Photographs taken for SIMS PUPILS: information relating to academic progress and test/exam results, general low-level safeguarding concerns, general information about personal circumstances (where not deemed to be highly sensitive), disciplinary/behaviour records. Individual photos and photos taken for SIMS.
High or 'Special Category Data'	EVERYONE: CCTV footage Potentally embarrassing/distressing/damaging Information about someone's private life PUPILS: Biometric data records, non-health or sexuality related safeguarding concerns STAFF: Salary details, Bank account details, NI Insurance numbers Disciplinary records, capability records, letters of concern Information relating to grievances, bullying or harassment. DBS certificates, medical questionnaires Maternity Risk assessments Health records PARENTS: Bank account details. Information relating to personal financial circumstances. Complaints may be highly sensitive depending on nature.
Special Category Data (extremely high sensitivity profile)	EVERYONE: All health records including sickness absence data (where a medical reason is noted for absence) and sick notes Risk assessments involving specific named individuals with medical issues (Information about allergies or certain medical conditions (e.g. epilepsy, diabetes) can be communicated to other members of staff quite widely where this is reasonably necessary to protect someone's health)

	Information relating to somene's belief race; ethnic origin; politics; religion; trade union membership; genetics; sex life; or sexual orientation. PUPILS: Biometric data records (where fingerprinting is used for registration) information relating to a pupil's religion such as records of baptism, confirmation and first holy communion (including photographs of ceremonies), information relating to Special Educational Needs, and disabilities, or other health conditions. May include Safeguarding information where concerns involve health, sex-life or sexuality. STAFF: completed medical questionnaires, sick notes, sickness absence records where reason for absence is logged. Maternity risk assessments. Medical records and reports.

Sharing Personal Data

External Data Sharing

If you are sharing an individual's personal data ***outside*** of Stonyhurst you need to ensure that the sharing of that data complies with the law and meets an individual's expectations.

Special category data should not generally be shared outside of Stonyhurst unless you have specific consent from a data subject (or their parent/s, where a data subject is a child) or where it is necessary to give a healthcare professional medical information in an emergency. In any other situation, advice should be sought first from Stonyhurst's Legal Adviser.

Other data should usually only be shared without the express permission of an individual *if* the individual has been informed about it through our Privacy Notice. Our Privacy Notice (available on the homepage of our website) informs our community of how we use people's personal data and who we share it with. Even then, when sharing personal data we should ensure that the sharing is justified and that we are not sharing more personal data than we ought to be; for example, if an organisation legitimately requires us to provide them with someone's date of birth only, we should not also be providing their place of birth. The data we provide should always be restricted to only what is truly essential.

The two following checklists provide a handy step-by-step guide through the process of deciding whether to share personal data. One is for systematic data sharing, the other is for one-off requests. In both cases, however, you should always ask yourself the following questions:

Is the person who is asking for the information definitely who they say they are? Have we initiated the contact or have they? Have we had contact with them before? Is the email address that we are sending the information to the same as the email address we have on file? Don't just assume that someone is who they say they are when they are asking you for personal information (including your own personal information).

Should you take extra security measures because of the nature of the information which you are sharing? Once you have established that the intended recipient to an email is entitled to the personal information, consider whether you should take any additional measures to protect the information. The measures you take should be directly proportionate to the volume of data you are sending and the sensitivity profile of the data. If you are sending large amounts of personal data (even where you have assessed the personal data as having a low sensitivity profile) you should ensure that this is encrypted. If you are sending 'special category data' such as information relating to health (which would include any SEN records and safeguarding/child protection information specific to a pupil), or other highly sensitive data (see grid above for examples) this must always be encrypted even if sending just one record/piece of information. You should use your professional

judgement on whether to encrypt smaller amounts of data of low/medium sensitivity, having regard to what the information is and who you are sending it to. If you are not sure, speak to your Line Manager, or err on the side of caution and encrypt it anyway. **Our ICT department will be able to assist in arranging encryption.**

Data Sharing

You should use the data sharing checklists below to decide whether you should be sharing personal data outside of Stonyhurst. Please speak to the Legal Adviser if you have any doubts.

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals (taking into account the sensitivity profile of the data) and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- Does the information include any special category information or highly confidential information? If so check whether we have consent to share information in this way or consider whether an individual is at risk of harm if we do not share this information. Seek advice from your line manager, the legal adviser or the Bursar if you are not sure.
- Any relevant functions of the organisation
- The nature of the information you have been asked to share (for example was it given in confidence?)
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

- If we are not legally obliged to provide the data we must make sure we have a data sharing agreement in place. The agreement should cover:
  - What information needs to be shared
  - The organisations that will be involved
  - What you need to tell people about the data sharing and how you will communicate that information
  - Measures to ensure adequate security is in place to protect the data
  - What arrangements need to be in place to provide individuals with access to their personal data if they request it
  - Agreed common retention periods for the data
  - Processes to ensure secure deletion takes place

If we don't have a suitable data sharing agreement in place speak to the Legal Adviser.

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the legislation to share?(Speak to the Legal Adviser if you're not sure)

Do you have the power to share?

Key points to consider:

- Does the information include any special category information or highly confidential information? If so check whether we have consent to share information in this way or consider whether an individual is at risk of harm if we do not share this information. Seek advice from your line manager, the Legal Adviser or the Bursar if you are not sure.
- Any relevant functions of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Internal Access to Personal Data

It is the responsibility of line managers and department Heads to ensure that personal information created or collected within their particular department is accessed only by members of staff who

have a legitimate need to access that information. Line managers and Heads of Department should be particularly careful to ensure that where a personal record contains special category data, or other highly sensitive personal information, the special category information is withheld from general departmental access unless there is clear justification for sharing that type of data. Access to special category data or highly sensitive data must be on a 'need-to-know' basis only. This does not neccarily mean that information, particularly medical information or Special Education Needs information cannot be widely known among staff, it just means that where staff do know about it, there must be a good reason for them to have that information.

Data Security

All staff are responsible for ensuring that they protect any personal information which they become privy to during their employment at Stonyhurst. All personal data should be protected, but particular care needs to be taken to protect special category data, or data which, if it fell into the wrong hands, could be especially detrimental or embarrassing, including bank account details or details about someone's private life.

Protecting Electronic Data

- Line managers are responsible for ensuring appropriate access to data on the departmental shared network, liaising, if necessary, with the ICT department.
- Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data – or any large quantity of data – should ***as a minimum*** be password-protected and held on a limited number of devices where possible, with passwords provided on a need-to-know basis and regularly changed.
- All members of staff who access Stonyhurst personal information (via the Stonyhurst network, their Stonyhurst email accounts, or any other applications or software which contain personal information which has been processed by Stonyhurst) through their personal electronic devices (smartphones, tablets or computers) must comply with the Bring Your Own Device Policy and ensure that they maintain appropriate security measures on their device which must include strong password protection.
- A 'strong' password should be at least six characters (although the more characters the stronger the password) and should contain a variety of upper case and lower case letters, numbers and symbols. Make sure that your passwords do not contain user names or real names. Ideally, your passwords should not contain complete words and they should be significantly different to each other. Do not write your password down. If you need to provide a purely numerical passcode, do not use your date of birth or your telephone number (nor should you use the date of birth or telephone number of someone close to you).
- Always remember to sign out of all applications when you exit them and do not let a device 'remember your password' for an application which contains Stonyhurst personal information.
- Always log out of your computer if you are leaving it unattended, particularly if you are working in an area which is accessible to pupils or visitors
- Do not put ***any*** personal information relating to Stonyhurst on a memory stick, unless that memory stick is encrypted and the Bursar has given written permission for an encrypted memory stick to be used.
- **Any existing unencrypted memory sticks which contain personal data must be handed to your head of department as soon as possible so that the information can be either deleted or transferred to the Stonyhurst network.**
- Personal devices and Stonyhurst-owned devices, where they allow access to Stonyhurst personal information should be kept securely and should not be left unattended in an

unsecured environment. Such devices should not be left in vehicles unless absolutely necessary in which case the vehicle must be locked and the devices must be put out of sight, if possible into a locked boot. Devices allowing access to Stonyhurst data must not be left unattended in a vehicle overnight.

- If you use an electronic device to access Stonyhurst personal data and it is lost or stolen, report the loss to the ICT department and the Bursar ***as soon as possible***.

Emails

- Emails (whether they are retained electronically or printed out as part of a paper file) are also "records". The format is secondary to the content and the purpose of keeping the document as a record. Therefore, when considering how long to keep an email for, reference should be made how long that category of data should be kept for, in accordance with our retention policies. Line managers should stipulate how and/or where they wish emails to be organised within their department.
- **Emails are often the source of major accidental data protection breaches**. Whilst we can put in place organisational measures to protect our personal information (through the use of pass-word protection, encryption, locks etc), as an organisation we cannot as easily prevent members of staff accidentally disclosing personal information either by basic error or as a result of a third party's deception. **We therefore rely on your professional judgement, vigilance and attention to detail at all times.**
- When sending emails to more than one external email recipient, always remember to put the recipient email addresses in the blind copy (Bcc) field. Be particularly careful when you are transferring email addresses from a spreadsheet to a recipient field. If you put the email addresses into the Cc: or To: fields, then all recipients will be able to see the other recipients' email addresses which will be a breach of existing data protection legislation and, under the new Regulations, may result in a significant fine. Check, re-check, and check again. Once you press 'send' it is too late to rectify a mistake.
- Be careful when sharing personal information with any outside organisation or individual and follow the guidance set out above in the Data Sharing section.
- Even when sending internal emails, if you are sending information containing personal data (particularly the names and other personal information of pupils) think about whether the recipients to the email have a legitimate reason to be given the information in your email. Whilst it may be easier to send an email to 'all staff' than to select particular email distribution groups, you should be asking yourself the question 'do all staff at Stonyhurst need to know this?', if the answer is 'no', then you should take the time to select the appropriate email recipients.
- Be careful not to 'reply to all' by accident. If this is set as your default reply option then speak to the ICT department who will be able to change it to 'reply'.
- Remember always that anytime you refer to an individual in an email (whether you are writing to them personally or you are writing about them to someone else) you are creating 'personal data' which, under data protection legislation, they may have a right to access. If you are considering putting sensitive information or opinions about someone (colleague, parent or pupil) in an email to another person, make sure your email is entirely professional and does not make baseless assumptions; make sure that you would be willing to stand by your email if you were challenged. Always follow our email protocol and remember that your email may, at some point in the future, be seen by the individual who you are writing about, or by a court of law. Be aware too that sending unprofessional emails may result in disciplinary action.
- Sometimes it is a good idea to put things in writing so you can rely on it later, but if you are in doubt, avoid putting sensitive information in an email and speak to someone face to face or over the phone. Use your professional judgement.

Hard Copy Data

Under the legislation, paper or other hard copy records of personal information are only classed as 'personal data' if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. It is good practice, however, to protect all hard copy data in the same way (even if it is not caught by data protection legislation we still have a duty to keep information confidential where appropriate).

Note that, when personal information is contained on print-outs taken from electronic files, this data has ***already been processed*** by the school and falls under the legislation. Remember: Data Protection is only one consideration in retaining records, so it is preferable to keep paper documents ordered and accessible.

In order to protect hard copy data, staff should:

- Only put personal data on central displays/on walls/on centrally accessible lists where the personal data has a low sensitivity profile OR where the information is necessary for a health and safety reason (in which case it should usually only be visible to staff members only).
- Ensure that personal data should otherwise be kept in a filed or otherwise orderly manner. The appropriate level of security afforded to hard copy data will depend on its nature. Personal information should ideally be held in cabinets (which are locked when not in use), or otherwise in offices which are locked when empty. Particular care is required if information is located in a place which is sometimes accessible to visitors or pupils (without staff supervision), in which case information must always be kept in locked filing cabinets when unattended, even if only unattended for a minute.
- Make sure that special category data and highly sensitive personal data is always be kept in filing cabinets which are locked when unattended, and that only authorised individuals who have a genuine need to see the information are given the keys.
- Not take hard copy personal information home unless they have good reason to do so, but if they do they must ensure that the data is kept as securely as possible whilst off-site, and is returned to Stonyhurst as soon as possible. If you are unable to ensure that the information is kept secure whilst in your possession then you should not take it off-site. Personal data must not be kept off-site indefinitely. Members of staff are only allowed to take 'special category data' or highly sensitive data off-site where there is a necessary health and safety reason for doing so (e.g. taking medical information/consent forms on a school trip) or where they have been given express permission by their line manager/Head of Department.
- Not leave hard copy personal information unattended in a vehicle unless absolutely necessary, in which case the vehicle must be locked and the personal information must be kept out of sight, if possible in a locked boot. Personal information must not be left unattended in a vehicle overnight.
- Collect your printing without delay if you have printed out any personal data, or use your mail box facility.
- Not leave personal data lying about on desks, or elsewhere, where it is visible to other members of staff, pupils or visitors.
- Consider the way in which paper records are stored, especially if they are going in to archiving or are otherwise likely to be stored for a considerable length of time. Paper records are most often damaged by damp or poor storage conditions; the optimal storage conditions are dry

and cool with reasonable ventilation and no direct sunlight; and paper should not be stored next with metals, rubber or plastic which might deteriorate or damage the paper.

CCTV Footage

CCTV footage is the personal data of the indviduals whose images are caught on camera. Members of staff who, as part of their role, are involved in managing the CCTV system, monitoring the CCTV footage, or installing or repositioning the cameras must read and comply with the CCTV policy.

Taking, Using and Storing Images of Pupils policy

Just as CCTV footage is personal data, so too are other images of individuals. For that reason, images of individuals should be treated like any other piece of personal data. For safeguarding reasons, however, we have more reason to be particularly protective of pupil's images. Any member of staff taking photos or videos of pupils (other than when that photograph is taken for legitimate domestic purposes, such as where the photo is of a family member) must read and comply with our Policy on Taking, Storing and Using Images of Pupils.

Data Retention

In the light of the Independent Inquiry into Child Sexual Abuse and various high-profile safeguarding cases, all independent schools will be aware of the emphasis currently being placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting.

It is strongly to be recommended in the current climate that we do **not** embark on a policy of deleting historic staff and pupil files, or any material potentially relevant for future cases, even if it has been held for long periods already. **Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.**

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

Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

RETENTION PERIODS

Type of Record/Document	**Retention Period**
SCHOOL-SPECIFIC RECORDS • Registration documents of School • Attendance Register • Minutes of Governors' meetings • Annual curriculum	
INDIVIDUAL PUPIL RECORDS • Admissions: application forms, assessments, records of decisions • Examination results (external or internal) • Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records • Special educational needs records (*to be risk assessed individually*)	***NB – this will generally be personal data*** 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision). 7 years from pupil leaving school ALL: 25 years from date of birth (subject where relevant to safeguarding considerations). Any material which may be relevant to potential claims should be kept for the lifetime of the pupil. Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely.

CORPORATE RECORDS (where applicable)	
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
• Shareholder resolutions	Minimum – 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
• Annual reports	Minimum – 6 years
ACCOUNTING RECORDS	
• Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*)	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements

• Tax returns	Minimum – 6 years
• VAT returns	Minimum – 6 years
• Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)
• Contracts of employment	7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme

• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years
• Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
• Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years
ENVIRONMENTAL & HEALTH RECORDS	
• Maintenance logs	10 years from date of last entry
• Accidents to children	25 years from birth (unless safeguarding incident)
• Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances	Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.

Data destruction

Line managers must ensure that all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Subject Access Requests

A subject access request is a written request from an individual (a 'subject') to receive copies of any personal information which we hold about them. This will include information held in files, or held electronically including on our network and on emails. The request can be by letter or email, or could even via social media, and it does not have to identify itself as being a 'Subject Access Request'.

Subject access requests must be processed within 30 days and there are fines for failing to respond. There are also risks associated with responding if the documents which we disclose show that we acted unprofessionally, unlawfully or negligently, as this may result in damage to our reputation or may give rise to successful legal action.

Please note that, following the receipt of a subject access request, we may be required to conduct a search of your email account in order to find any emails which we may be obliged to disclose. Whilst you will usually be advised of this, it may not be possible to give you advance notice on some occasions. We may also withhold the name of the person who has made the subject access request if we feel it is appropriate. Please also note that whilst we will be obliged to redact third party names when disclosing personal information as part of a subject access request (such as the names of pupils and parents), we will not normally redact staff names unless the information relating to that staff member is considered to be particularly sensitive.

If you receive a subject access request then you must forward this to the Bursar immediately. Subject Access Requests often involve complicated legal issues and if they are not dealt with properly could result in legal action against us or data protection breaches. Do not respond to a Subject Access Request yourself unless you have been given authorisation to do so by the Bursar or Legal Adviser.

Other Requests from Data Subjects

We may occasionally receive requests from individuals to delete, amend or stop using their personal data. If you receive such a request you should refer this to your line manager, who may, in turn, may wish to discuss the matter with the Bursar or Legal Adviser. Do not give any assurances to anyone that we can agree to their request until you are sure that this is the case, although note that in the case of anyone asking us to stop contacting them where we are engaged in trying to sell services to them or engage them in fundraising activities, then we should ensure that we do not contact them again for those purposes.

Data Security Breaches

Data breaches occur when personal data is lost or stolen, or when it has been deliberately or accidentally disclosed to someone who does not have a right to see it. Examples would include where a memory stick has been lost, a laptop has been stolen or an email containing personal data has been sent to the wrong person.

It is absolutely crucial that you report any breaches or suspected breaches to the Bursar **as soon as is practicably possible**, whether or not you have made the mistake. Once a breach has happened you will only make the situation worse by not reporting it. Under the new legislation we have to report breaches to the Information Commissioner '**without undue delay and, where feasible, not later than 72 hours after having become aware of it'**.

When reporting the breach to the Bursar, you must co-operate with any requests for additional information and you must provide this information as a matter of urgency.

We recognise that accidents happen and that mistakes are made, but we will not accept any attempt to deliberately cover up a breach.

Any Questions?

If you have any questions about this policy, or if you have any general concerns about data protection and its impact on your department then please contact the Bursar as soon as possible.