Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

DATA PROTECTION POLICY (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

1. Background

Data protection is an important legal compliance issue for West Buckland School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's [Privacy Notice]. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

The Data Protection Act 1998 changed on 25th May 2018 in light of the General Data Protection Regulation (GDPR). This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely.

While this new law does set out useful legal grounds in this area, in most ways this new law is strengthening the rights of individuals and placing tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and has powers to take action for breaches of the law. Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. This policy may be amended at any time.

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

Key data protection terms used in this data protection policy are:

- Data controller – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal information (or personal data): any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still

personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

2. Data Protection Officer

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

3. The Principles

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

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

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

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

4. Lawful grounds for data processing

Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.
One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Policy, as GDPR requires.

Other lawful grounds include:

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

5. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that your personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data Handling

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

- Safeguarding.
- Acceptable User Agreement.
- Privacy Notice.
- Retention and Disposal of Records.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.
Avoiding, mitigating and reporting data breaches
One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

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

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

Care and Data Security

More generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend and/or complete on-line training and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.
We expect all those with management/leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Assistant Bursar and to identity the need for (and implement) regular staff training.

6. Rights of Individuals

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

communication from an individual about their personal data), you must tell the Assistant Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Assistant Bursar as soon as possible.

7. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. When staff take data, on an electronic memory stick offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

8. Processing of Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Finance Officer.

9. Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

DATA RETENTION AND DISPOSAL

1. GDPR and Document Retention

General Data Protection Regulations (GDPR), from 25th May 2018, do not fundamentally change the principles for length of document retention – it is still a question of relevance and purpose, as well as data security.

It does, however, have stricter rules about use and storage of personal data generally with the practical effect of requiring more dynamic, efficient and secure storage systems. Notably:

- All information held by schools needs to be justifiable, by reference to its purpose.
- Schools must be transparent and accountable as to what they hold.
- Schools must understand and explain the reasons why they hold data – which also means keeping records that explain how decisions around personal data are made.
- Schools must be prepared to respond more quickly to subject access requests.
- Schools must be able to amend, delete or transfer data promptly upon any justified request, or otherwise prepared to explain why they will not.
- It should be possible to audit how your personal data was collected and when.
- Sensitive data must be held securely, accessed only by those with reason to view it, and schools should have an "appropriate policy document" as to why it is needed.

More information about the above is contained in the on-line training GDPR package which all staff are required to complete annually.

For the external audience, more details are contained in the School's Privacy Notice.

The GDPR requirement for School's to document their processing activities (i.e. to keep a record of what they do and why) has been covered in the School's Data Audit conducted just prior to the implementation date of GDPR.

2. IICSA, Child Protection and Document Retention

Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

Background. In the light of the Independent Inquiry into Child Sexual Abuse (IICSA), former Chair Dame Lowell Goddard's forceful statements, 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. Many will be extending this rule to all personnel and pupil files on a 'safety first' basis.

Historic Abuse Data Retention. This policy has been drafted in full awareness of these considerations. Accordingly, West Buckland School will not embark on a policy of deleting historic staff and relevant 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.

However, the present focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are now in suspension, nor that we may not still be liable for breaches of data protection legislation (such as retaining personal data longer or in greater volume than *is necessary for its purpose*, or a failure to keep the data accurately or safely).

Clearly, we should have a lifetime retention of records where they are of potential relevance to historic abuse cases. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not), or details as to physical or mental health, should be kept securely and shared or accessible only on a need-to-know basis.

Striking a balance

Even justifiable reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the school will need to be weighed against personal rights. The longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative burden on schools, in terms of both secure storage and individual subject access rights.

This policy provides the School's interpretation of the balance to be struck at West Buckland School.

Meaning of "Record"

A "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 DPA.

An obvious example of personal data would be the Single Central Record or a pupil file; however, a "record" of personal data could arise simply by holding an email on the school's systems.

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.

Digital records

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 only, with passwords provided on a need-to-know basis and regularly changed. Where 'cloud storage' is used, consider what data needs to be made available in this way. If personal information kept in this way is sensitive, or held in large quantities, digital encryption is advisable.

Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record.

It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes: so it is important that this information is preserved.

Paper records

Paper records are most often damaged by damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital – especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.

Under the DPA, paper records 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.

However, 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 DPA. Remember: the DPA is only one consideration in retaining records, so it is preferable to keep paper documents ordered and accessible.

2. Archiving and the destruction or erasure of Records

All staff will receive basic training in data management – issues such as security, recognising and handling sensitive personal data, safeguarding etc. Staff will be given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- That records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks,

or mobiles and handheld electronic tablets) unless absolutely necessary, *in which case* it should be subject to a risk assessment and in line with an up-to-date IT use policy;

- That questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual *ad hoc* action;

- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements providing for security and access;

- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and

- 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.

This is particularly important in respect of the school's specific legal obligations under the DPA. However, they amount to common sense rules even where personal data is not directly involved.

4. A note on litigation

One consideration in whether it is necessary or desirable to keep records is possible future litigation. Generally speaking, an institution will be better placed to deal with claims if it has a strong corporate memory – including adequate records to support its position, or a decision that was made.

Ideally, therefore, records would not be disposed of until the limitation period for bringing a claim has passed. For most contracts that will mean 6 years from any breach (or 12 years in case of, say, a witnessed deed), but the date to start counting from is the last day of the period under contract. Where there has been early termination, this will be the relevant date to apply (once the appeal process has been concluded): but for pupils, limitation periods will only apply from the age of 18 years.

The period of 6 years also applies to many claims outside contract (such as fraud, mistake or negligence). For discrimination cases it is usually only 3 months. In the case of personal injury, and some other negligence claims, it is 3 years. However, if the harm is only discovered later – eg 'latent' damage, or some unseen injury – then the timer only starts from the point of discovery: subject, in the case of latent property damage, to a 15-year backstop.

In some cases the prompt may be the end of a calendar year, so for the purpose of this guidance a contingency is generally built in (eg 7 years where the statutory limitation is 6 years).

Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (eg historic abuse), whether a charge is brought by the police or a school

is sued under a private claim. It is not always possible to try a case where the evidence is inadequate, including due to a lack of corporate memory (eg records and witnesses). However, as recent cases and IICSA (the Independent Inquiry into Child Sexual Abuse) have shown, authorities will expect to see a full and proper record and inferences may be drawn otherwise.

Often these records will comprise personal or sensitive personal data (eg health or criminal allegations). In such instances, even justifiable reasons to keep records for many years will need to be weighed against personal rights. Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a DPA perspective, make it easier for a school to justify retention for long periods – even the lifetime of a pupil. The most important steps a school can take to support such a policy are (a) having adequate policies explaining the approach, including notices in both staff and parent contracts; and (b) ensuring any long-term records worth keeping are kept very secure, accessible only by trained staff on a need-to-know basis.

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise.

5. The risks of longer retention

Notwithstanding the legal grounds and (in some cases) imperatives to do so, the longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden on schools. This also increases the amount of material in respect of which schools must be accountable to data subjects (e.g. information requests, "right to be forgotten" requests), and the consequences of data security breach become more serious.

Schools must take professional advice and decide for themselves where to draw the line in retaining data for these purposes: some may err on the side of caution and retain; others will apply a clear system for filleting pupil or personnel files, or indeed email folders, down to the information they think is likely to be relevant in the future. However, this is a decision that should always be made mindful of risk and knowledge of where historic incidents may have occurred or future complaints may arise.

It is also vitally important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request under the DPA. The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity.

6. A note on secure disposal of documents

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.

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.

How to use the table of suggested retention periods

The table at the end of this guidance document has three main functions:

- it should help schools and staff identify the key types of document concerned.
- it should focus attention on any particular issues associated with those types of document.
- finally – and this needs to be emphasised – it acts as an outline guide only.

Note that, except where there is a specific statutory obligation to destroy records, it is misleading to present (or apply) any guidance as if it constitutes prescriptive time 'limits'. Figures given are not intended as a substitute to exercising thought and judgment, or take specific advice, depending on the circumstances.

Indeed, the essence of this guidance can be boiled down to the necessity of exercising thought and judgment – albeit that practical considerations mean that case-by-case 'pruning' of records may be impossible. It is accepted that sometimes a more systemic or broad-brush approach is necessary, which is where the table comes in.

RETENTION PERIODS

Type of Record/Document	**Suggested [1] Retention Period**
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)

Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

INDIVIDUAL PUPIL RECORDS	***NB – this will generally be personal data***
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).
• Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	***NB – please read notice at the top of this note***
• 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. [2]
• 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. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).

CORPORATE RECORDS (where applicable)	**e.g. *where schools have trading arms***
• 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 [3]	
• 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*) [NB specific ambit to be advised by an accountancy expert]	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 eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will contain personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
• 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

Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

ENVIRONMENTAL, HEALTH & DATA	
• Maintenance logs	10 years from date of last entry
• Accidents to children [4]	25 years from birth (longer for safeguarding)
• Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event or activity.
• Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)

FOOTNOTES:

1. General basis of suggestion:

Some of these periods will be mandatory legal requirements (eg under the Companies Act 2006 or the Charities Act 2011), but in the majority of cases these decisions are up to the institution concerned. The suggestions will therefore be based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (eg every 6 years) in place.

3. Retention period for tax purposes should always be made by reference to specific legal or accountancy advice.

4. Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this: so keep a note of all procedures as they were at the time, and keep a record that they were followed. Also keep the relevant insurance documents.

Policy: Data Protection (INCLUDING DATA RETENTION, STORAGE AND DISPOSAL)

Author/Updated by: Bursar Date: 16 Jan 2015
Reviewed: 4 Jan 2016
Reviewed: 30 June 2017
Reviewed: 28 Sep 18
ISBA 2018 Template used to update ensure GDPR Compliant.
Next Review Date: Summer 2020