Data Protection Policies and Guidance

Approved by: Karen Pickles
Designated Safeguarding Lead

Date: 15th September 2023

POLICY REVISION RECORD (annual reviews)

Date	Section	Revision/review	Updated by
25/05/2019			Karen Pickles
26/05/2020		Additional helpline added	Karen Pickles
18/06/2021			Karen Pickles
24/06/2022			Karen Pickles
14/09/2023	Re-written policy	Updated and re-styled to include all above as required and reviewed for GDPR requirements 2023: Separating staff and pupil/parent privacy.	Karen Pickles

Staff Privacy Policy

This document is applicable to past and present staff and homestays of Berkeley Guardians

In the course of your employment, engagement or other basis of work undertaken for Berkeley Guardians, we will collect, use and hold ("process") personal data relating to you as a member of our staff. This makes the Guardianship a data controller of your personal information, and this Policy sets out how we will use that information and what your rights are.

To whom the document applies:

Homestays, office staff, guardian angels and others who may be employed or engaged by the Guardianship to work for it in any capacity, as well as prospective applicants for roles.

About this document:

This policy explains how the Guardianship collects, uses and shares (or "processes") personal data of staff, and your rights in relation to the personal data we hold.

This policy also applies in addition to the Guardianship's other relevant terms and conditions and policies, including:

- any contract between the Guardianship and its staff, such as the terms and conditions of employment, and any applicable staff handbook
- the Guardianship's retention of records policy;
- the Guardianship's safeguarding, pastoral, anti-bullying, or health and safety policies, including as to how concerns or incidents are reported or recorded (both by and about staff)
- the Guardianship's IT policies, including its Acceptable Use policy and e-Safety policy.

  Please note that your contract with the Guardianship, including any document or policy forming a part of your contractual obligations to the Guardianship, may in particular be relevant to and supplement the information in this policy, to the extent that it will contain details of obligations or rights of the Guardianship under contract with you which may require the use of your personal data. However, this policy is the primary document applicable to the use of your personal data by the Guardianship.

This policy also applies alongside any other information the Guardianship may provide about particular uses of personal data, for example when collecting data via an online or paper form.

Responsibility for data protection:

The Designated Safeguarding Lead will deal with all your requests and enquiries concerning the Guardianship's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

How we collect your information:

We may collect your personal data in a number of ways, for example:

- from the information you provide to us before making a job application, for example when you come for an interview
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, etc.
- from third parties, for example the Disclosure and Barring Service (DBS) and referees (including your previous or current employers), in order to verify details about you and/or your application to work for us

More generally, during the course of your employment with us, as a member of staff, we will collect data from or about you, including:

- when you provide or update your contact details
- when you or another member of staff completes paperwork regarding your performance appraisals
- in the course of fulfilling your employment (or equivalent) duties more generally, including by filling in reports, note taking, emails sent
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

The types of information we collect:

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

- contact and communications information, including:
    - your contact details (including email address(es), telephone numbers and postal address(es)
    - contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this policy
    - records of communications and interactions we have had with you
    - biographical, educational and social information, including:
        - your name, title, gender, nationality and date of birth
        - your image and likeness, including as captured in photographs taken for work purposes
        - details of your education and references from your institutions of study
        - lifestyle information and social circumstances
        - your interests and extra-curricular activities
        - financial information, including:
            - your bank account number(s), name(s) and sort code(s) (used for paying your salary and processing other payments)
            - your tax status (including residence status)
            - information related to pensions, national insurance, or employee benefit schemes
        - work related information, including:
            - details of your work history and references from your previous employer(s)
            - your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the Guardianship

- details of your professional activities and interests
- your involvement with and membership of sector bodies and professional associations
- information about your employment and professional life after leaving the Guardianship, where relevant (for example, where you have asked us to keep in touch with you)
- and any other information relevant to your employment or other engagement to work for the Guardianship

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

- information revealing your racial or ethnic origin
- trade union membership, where applicable
- information concerning your health and medical conditions (eg., where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
- information concerning your sexual life or orientation (eg., in the course of investigating complaints made by you or others, eg. concerning discrimination)
- information about certain criminal convictions (eg., where this is necessary for due diligence purposes, or compliance with our legal and regulatory obligations)

However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for the School.

The bases for processing your personal data, how that data is used and with whom it is shared:

(i) Entering into, or fulfilling, our contract with you

We process your personal data because it is necessary for the performance of a contract to which you are a party or to take steps at your request prior to entering into a contract, such as a contract of employment or other engagement with us. In this respect, we use your personal data for the following:

- administering job applications and, where relevant, offering you a role with us
- carrying out due diligence checks on you, whether during the application process for a role with us or during your engagement with us, including by checking references in relation to your education and your employment history
- once you are employed or engaged by us in any capacity, for the performance of the contract of employment (or other agreement) between you and us
- to pay you and to administer benefits (including pensions) in connection with your employment or other engagement with us
- monitoring your attendance and your performance in your work, including in performance appraisals
- promoting the Guardianship to prospective parents and others, including by publishing the work product(s) you create while employed by or otherwise engaged to work for the Guardianship
- for disciplinary purposes, including conducting investigations where required

- for other administrative purposes, for example to update you about changes to your terms and conditions of employment or engagement, or changes to your pension arrangements
- for internal record-keeping, including the management of any staff feedback or complaints and incident reporting
- for any other reason or purpose set out in your employment or other contract with us

(ii) Legitimate Interests

We process your personal data because it is necessary for our (or sometimes a third party's) legitimate interests. Our "legitimate interests" include our interests in running the Guardianship in a professional, sustainable manner, in accordance with all relevant ethical, educational, legal and regulatory duties and requirements (whether or not connected directly to data protection law).

In this respect, we use your personal data for the following:

- providing you with information about us and what it is like to work for us (where you have asked for this, most obviously before you have made a formal application to work for us)
- to enable relevant authorities to monitor the Guardianship's performance and to intervene or assist with incidents as appropriate
- to safeguard pupils' welfare and provide appropriate pastoral care
- to carry out or cooperate with any school, guardianship or external complaints, disciplinary or investigatory process
- for the purposes of management planning and forecasting, research and statistical analysis
- in connection with organising events and social engagements for staff
- making travel arrangements on your behalf, where required
- contacting you or your family members and 'next of kin' for business continuity purposes, to confirm your absence from work, etc.
- publishing your image and likeness in connection with your employment or engagement with us

(iii) Legal Obligations

We also process your personal data for our compliance with our legal obligations, notably those in connection with employment, company law, tax law and accounting, and child welfare. In this respect, we use your personal data for the following:

- to meet our legal obligations (for example, relating to child welfare, social protection, diversity, equality, and gender pay gap monitoring, employment, and health and safety)
- for tax and accounting purposes, including transferring personal data to HM Revenue and Customs to ensure that you have paid appropriate amounts of tax.
- for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

(iv) Special categories of data

We process special categories of personal data (such as data concerning health, religious beliefs, racial or ethnic origin, sexual orientation or union membership) or criminal convictions and allegations for the reasons set out below.

We will process this data on the basis that such processing is necessary to carry out obligations and exercise rights (both yours and ours) in relation to your employment.

In particular, we process the following types of special category personal data for the following reasons:

- your physical or mental health or condition(s) in order to record sick leave and take decisions about your fitness for work, or (in emergencies) act on any medical needs you may have
- recording your racial or ethnic origin in order to monitor our compliance with equal opportunities legislation
- trade union membership, in connection with your rights as an employee and our obligations as an employer
- categories of your personal data which are relevant to investigating complaints made by you or others, for example concerning discrimination, bullying or harassment
- data about any criminal convictions or offences committed by you, for example when conducting criminal background checks with the DBS, or where it is necessary to record or report an allegation (including to police or other authorities, with or without reference to you)

We will process special categories of personal data for lawful reasons only, including because:

- you have given us your explicit consent to do so, in circumstances where consent is appropriate
- it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention
- it is necessary for some function in the substantial public interest, including the safeguarding of children or vulnerable people, or as part of a process designed to protect others from malpractice, incompetence or unfitness in a role (or to establish the truth of any such allegations)
- it is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you

Sharing your information with others

For the purposes referred to in this policy and relying on the bases for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

- other employees, agents and contractors (eg third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
- DBS and other relevant authorities and agencies such as the Department for Education, the ICO, Company House and the local authority

- external auditors or inspectors
- our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants
- third parties and their advisers in the unlikely event that those third parties are acquiring or considering acquiring all or part of our Guardianship, or we are reconstituting
- when the Guardianship is legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations.

How long your information is kept?

Personal data relating to unsuccessful job applicants is deleted with 12 months (minimum 3 months), except where we have notified you we intend to keep it for longer (and you have not objected).

For employees, subject to any other policies that we may provide to you, we may retain your personal data for a period of 7 years after your contract of employment (or equivalent agreement) has expired or been terminated.

However, some information may be retained for longer than this, for example incident reports and safeguarding files, in accordance with specific legal requirements. Please see Storage and Retention of Records and Documents Policy.

Your rights

Your rights as a 'data subject' are the same as if you were any member for the public. You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

This Policy

The Guardianship will update this policy from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Contact and complaints

If you have any queries about this policy or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you may contact your line manager or refer the matter through the staff grievance procedure.

If you are not satisfied with how we are processing your personal data, or how we deal with your complaint, you can make a complaint to the Information Commissioner: www.ico.org.uk. The ICO does recommend you seek to resolve any issues with the data controller initially prior to any referral.

Pupil and Parental Privacy Policy

This document is applicable to past and present pupils and parents of Berkeley Guardians Ltd.

This policy is intended to provide information about how the Guardianship will use (or "process") personal data about individuals including: its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This information is provided because Data Protection Law gives individuals rights to understand how their data is used. Staff, parents and pupils are all encouraged to read this policy and understand the Guardianship's obligations to its entire community.

This policy applies alongside any other information the Guardianship may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This policy also applies in addition to the Guardianship's other relevant terms and conditions and policies, including:

- any contract between the Guardianship and the parents of pupils
- the Guardianship's policy on taking, storing and using images of children
- the Guardianship's retention of records policy
- the Guardianship's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded
- the Guardianship's IT policies, including its Acceptable Use policy, e-Safety policy. Anyone who works for, or acts on behalf of, the Guardianship (including staff, and homestays) should also be aware of and comply with this policy.

Responsibility for data protection

The Designated Safeguarding Lead (Mrs. Karen Pickles) as Compliance Officer will deal with all your requests and enquiries concerning the Guardianship's use of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

Why the School needs to process personal data

In order to carry out its ordinary duties to staff, pupils and parents, the Guardianship needs to process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the Guardianship will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the Guardianship's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

The Guardianship expects that the following uses will fall within that category of its (or its community's) "legitimate interests":

- For the purposes of pupil applications (and to confirm the identity of prospective pupils and their parents)

- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity analysis)
- To enable relevant authorities to monitor the Guardianship's performance and to intervene or assist with incidents as appropriate
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils
- To safeguard pupils' welfare and provide appropriate pastoral care
- To monitor (as appropriate) use of the homestays' IT and communications systems in accordance with the Guardianship's Acceptable Use Policy
- To make use of photographic images of pupils in Guardianship publications, on the Guardianship website and (where appropriate) on the Guardianship's social media channels in accordance with the Guardianship's policy on taking, storing and using images of children
- To carry out or cooperate with any school, guardianship or external complaints, disciplinary or investigation process
- Where otherwise reasonably necessary for the Guardianship's purposes, including to obtain appropriate professional advice and insurance for the Guardianship

In addition, the Guardianship will on occasion need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to homestays who need to be made aware of dietary or medical needs

- As part of any Guardianship or external complaints, disciplinary or investigation process that involves such data, for example if there are health or safeguarding elements
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

Types of personal data processed by the Guardianship

This will include by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details
- bank details and other financial information, e.g. about parents who pay fees to the Guardianship
- past, present and prospective pupils' academic, disciplinary, applications records etc
- where appropriate, information about individuals' health and welfare, and contact details for their next of kin

- references given or received by the Guardianship about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils
- correspondence with and concerning pupils and parents past and present

How the Guardianship collects data

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data will be supplied by third parties (for example another School, or other professionals or authorities working with that individual); or collected from publicly available resources.

Who has access to personal data and with whom the Guardianship shares

Occasionally, the Guardianship will need to share personal information relating to its community with third parties, such as:

- professional advisers (e.g. lawyers, insurers, PR advisers and accountants)
- government authorities (e.g. HMRC, DfE, police or the local authority)
- appropriate regulatory bodies (e.g. AEGIS, BSA or the Information Commissioner)
- Homestays
- Photographers
- Health care service providers

For the most part, personal data collected by the Guardianship will remain within the Guardianship, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the Guardianship
- pastoral or safeguarding file

Staff, pupils and parents are reminded that the Guardianship is under duties imposed by law and statutory guidance (including ***Keeping Children Safe in Education***) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the Guardianship's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the Guardianship's processing activity is carried out on its behalf by third parties, such as cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the Guardianship's specific directions.

How long we keep personal data

The Guardianship will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the Guardianship. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If you have any specific queries about how our retention policy is applied or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Designated Safeguarding Lead. However, please bear in mind that the Guardianship will often have lawful and necessary reasons to hold on to some personal data even following such request.

A limited and reasonable amount of information will be kept for archiving purposes and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

For further information, please refer to the Guardianship's Storage and Retention of Records and Documents Policy.

Your rights

Rights of access, etc.

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the Guardianship, and in some cases ask for it to be erased or amended or have it transferred to others, or for the Guardianship to stop processing it – but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Designated Safeguarding Lead.

The Designated Safeguarding Lead will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information).

The Guardianship will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, the Guardianship may ask you to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).

Requests that cannot be fulfilled

You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by the Guardianship, or documents prepared in connection with a legal action).

You may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your (or your child's) personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this policy. All such requests will be considered on their own merits.

Pupil requests

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the Guardianship, they have sufficient maturity to understand the request they are making (*see section Whose Rights? below*). A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's: for older pupils, the parent making the request may need to evidence their child's authority for the specific request.

Pupils aged 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may however be sufficiently mature to have a say in this decision, depending on the child and the circumstances.

Parental requests, etc.

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The Guardianship may consider there are lawful grounds for sharing with or without reference to that pupil.

All information requests from, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

Consent

Where the Guardianship is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the Guardianship may not be relying on consent but have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this policy or may otherwise exist under some form of contract or agreement with the individual (e.g. *an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested*).

Whose rights?

The rights under Data Protection Law belong to the individual to whom the data relates. However, the Guardianship will often rely on parental authority or notice for the necessary

ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the Guardianship relying on strict consent (see section on Consent above).

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the pupil's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the Guardianship will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities and behaviour, and in the interests of the pupil's welfare. That is unless, in the Guardianship's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the Guardianship may be under an obligation to maintain confidentiality unless, in the Guardianship's opinion, there is a good reason to do otherwise; for example where the Guardianship believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the Guardianship's IT Acceptable Use Policy.

Data accuracy and security

The Guardianship will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the Designated Safeguarding Lead of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law): please see above for details of why the Guardianship may need to process your data, of who you may contact if you disagree.

This policy

The School will update this policy from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Queries and complaints

Any comments or queries on this policy should be directed to the Designated Safeguarding Lead – Mrs. Karen Pickles (email: karen@berkeleyguardians.com)

If an individual believes that the Guardianship has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise Berkeley Guardians complaints/grievance procedure and should also notify the Designated Safeguarding Lead. You can also make a referral to or lodge a complaint with the Information Commissioner's Office

(ICO), although the ICO recommends that steps are taken to resolve the matter with the Designated Safeguarding Lead before involving the regulator.

Storage and Retention of Records and Documents Policy

The following retention table sets out the Guardianship's policy on retention periods. The retention periods will be reviewed annually to ensure compliance with the law in force at that time.

Record or Retention Styles:

Emails on Server – *delete historic emails after 3 years* (unless a legal requirement is in place) but hold parental emails on file with pupil details for 7 years):

- Pupil email account
- Staff emails

Guardianship specific records – *delete after 7 years*

- Registration documents

Individual pupil records – *delete after 7 years*

- Admissions: application forms, medical forms etc.

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.

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

- Certificates of Incorporation
- Minutes, Notes and Resolutions of Management Meetings

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) to include:

- Tax returns
- VAT or Coporate Tax Returns

Contracts and Agreements

- Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)
- Deeds (or contracts under seal)

Intellectual Property Records

- Formal documents of title (trademark or registered design certificates; patent or utility model certificates)
- Assignments of intellectual property to or from the Guardianship
- IT agreements (*including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents*)

Employee Personal Records

- Single Central Record of employees
- Contracts of employment
- Employee appraisals or reviews
- Staff personnel file
- Payroll, salary, maternity pay records financial year in which the transaction took place
- Job application and interview/rejection records (unsuccessful applicants)
- Staff immigration records (Right to work, etc.)
- Tier 2 migrant worker sponsor records
- Health records relating to employees
- Low-level concerns records about adults (*unless safeguarding concerns and then keep for life)*

Delete all of above 7 years

Insurance Records

- Insurance policies (will vary – private, public, professional indemnity)
- Correspondence related to claims/ renewals/ notification re: insurance

Environmental Data

- Maintenance logs
- Accidents re pupils
- Accident at work records (staff)
- Staff use of hazardous substances
- Covid-19 risk assessments, consents etc. (*for now: this to be subject to further review*)
- Risk assessments (carried out in respect of above)

- Art.30 GDPR records of processing activity, data breach records, impact assessments

Minimum storage – 4 years from end of employment

Taking, Storing and Using Images of Children Policy

This Policy

This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Berkeley Guardians.

- It applies in addition to the Guardianship's terms and conditions, and any other information the Guardianship may provide about a particular use of pupil images, including e.g. signage about the use of CCTV; and more general information about use of pupils' personal data, e.g. the Guardianship's Privacy Notice. Images of pupils in a safeguarding context are dealt with under the Guardianship's relevant safeguarding policies.

General points to be aware of

- Certain uses of images are necessary for the ordinary running of the Guardianship; other uses are in the legitimate interests of the Guardianship and its community and unlikely to cause any negative impact on pupils. The Guardianship is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised
- Parents who apply for guardianship with Berkeley Guardians are invited to indicate agreement to the Guardianship using images of him/her as set out in this policy via the Guardianship's terms and conditions and/or from time to time if a particular use of the pupil's image is requested.
- However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example if they are included incidentally in CCTV or a photograph)
- Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Designated Safeguarding Lead in writing. The Guardianship will respect the wishes of parents and pupils wherever reasonably possible, and in accordance with this policy
- Parents should be aware that, from the age of 12 and upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images

Use of Pupil Images in Guardianship Marketing

Unless the relevant pupil or his or her parent has requested otherwise, the Guardianship reserves the right to use images of its pupils to keep the Guardianship community updated on the activities of the Guardianship, and for marketing and promotional purposes:

- in communications with the Guardianship community (parents, pupils, staff, homestays) including by email, on the Guardianship website and by post

- on the Guardianship's website and, where appropriate, via the Guardianship's social media channels, e.g. Twitter, Instagram and Facebook. Such images would not normally be accompanied by the pupil's full name without permission
- in the Guardianship's prospectus, and in online, press and other external advertisements for the Guardianship. Such external advertising would not normally include pupil's names and in some circumstances the Guardianship will seek the parent or pupil's specific consent, depending on the nature of the image or the use

The source of these images will predominantly be the Guardianship's staff (*who are subject to policies and rules in how and when to take such images*), or a professional photographer used for marketing and promotional purposes, or occasionally pupils. The Guardianship will only use images of pupils in suitable dress and the images will be stored securely and centrally.

Data Breach Procedure

This policy assumes that the criteria for reporting breaches to the ICO are understood -in short, this means that Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

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

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

They should be reported if the breach will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. If a report is required, caution will be taken with which organisation the data protection duty lies as Serious Incident reports are subject to Freedom of Information requests which may, if answered, create a further data or privacy breach if the lines of responsibility are not clear.