Data Protection Policy

Introduction

Heritage School is the main operating activity of Child Light Ltd (Company Number 2928829, Charity Number 1039099). The registered office of Child Light Ltd is 17-19 Brookside, Cambridge, CB2 1JE. For the purposes of Data Protection Law, Child Light Ltd (referred to in this policy as "the School") is the designated Data Controller.

Background

Data protection is an important legal compliance issue for Heritage 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, carers or guardians (referred to in this policy as "parents"), its contractors and other third parties (in a manner more fully detailed in the School's privacy notices - currently Recruitment Privacy Notice (on website); Staff Privacy Notice (INTERNAL); Parents, Pupils, Alumni and Friends of Heritage Data Privacy Notice (on website). The School, as data controller, is liable for the actions of its staff and trustees in how they handle data and keep data safe. 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 handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office ("ICO") is responsible for enforcing data protection law in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Definitions

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

- **Cyber Security** – refers to the practices and measures taken to protect computer systems, networks, and data from cyber threats, such as hacking, data breaches, and malware attacks.
- **Data Controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including the use of data by its trustees) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
- **Data Processor** – an organisation that processes personal data on behalf of a controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **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) by which that individual may be identified by the controller. Personal identifiers do not only include names but also include any other form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails,

notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

- **Processing** – virtually anything done with personal data, 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. This data is considered particularly sensitive and requires extra protection. Special category data can't be processed unless a controller can meet one of the exceptions in Article 9(2) of the GDPR. While not qualifying as special category data, there are also separate rules for the processing of personal data relating to criminal convictions and offences.

Virtually any information about a living person is likely to be personal data and examples are listed below:

- contact details and other personal information held about pupils, parents, prospective parents and staff and their families;
- information about a child protection incident;
- emails expressing opinion or intention in relation to a person;
- a record about disciplinary action taken against or an investigation into a member of staff;
- photographs, video images or voice recordings of pupils or staff;
- financial records;
- records of staff sickness absence or leave.

Application of this policy

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

Those who handle personal data as employees or trustees of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

Person responsible for Data Protection at the School

The Headmaster has overall responsibility for data protection and cyber security policy implementation and strategy.

The School has appointed the Compliance Officer as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. 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 Compliance Officer or Bursar.

The IT Manager is responsible for implementing technical controls, monitoring IT systems, responding to incidents and managing access and updates.

The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers and 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 UK GDPR's broader '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 (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); 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; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School 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 School. It can be challenged by data subjects and also means the School 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 Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- 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.

See Appendix 1 - Legal basis for processing information.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business digitally (most commonly in emails and documents) or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold/redact information from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask 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 Code of Conduct for Staff and all relevant School policies and procedures (to the extent applicable to them). 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 relevant to them:

- Staff Code of Conduct (all staff)
- Acceptable Use of IT Policy for Staff (all staff)
- Acceptable Use of Screens Policy (Teaching staff only)
- Preventing Extremism Policy
- Recruitment, Selection and Disclosure Policy (senior staff involved in recruitment only)
- Safeguarding Policy (all staff)
- Use of Images Policy
- Data Retention Guidelines.

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.

If you have access to personal data, you must:

- only access the personal data that you have authority to access, and only for authorised purposes;

- only allow others to access personal data if they have appropriate authorisation;
- keep personal data secure by complying to rules on access to premises, computer access, password protection, secure file storage and data retention and destruction;
- not remove personal data, or devices containing personal data (or which can be used to access it), from the School's premises unless appropriate security measures are in place (such as encryption or password protection);
- not store personal data on local drives (eg USBs) or on personal devices without express written permission of the Compliance Officer or Bursar;
- not use personal email accounts or unencrypted personal devices for official School business
- act in accordance with our Acceptable Use of IT Policy for Staff;
- not transfer data outside the EU without authorisation from IT and the Compliance Officer.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, 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 staff become aware of a personal data breach they must notify the Compliance Officer, the Bursar and IT. If staff are in any doubt as to whether to report something internally, 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 applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see "Application of this policy" section above), 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 affects other daily processes such as filing or sending out hard copy documents. Data handlers should always consider what the 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 Compliance Officer, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a Data Protection Impact Assessment (DPIA) before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Compliance Officer and IT in the first instance, and at as early a stage as possible.

For any sort of higher risk processing it will be necessary to complete a DPIA, carry out appropriate due diligence into the product, and ensure robust, GDPR-compliant contractual protections (including in respect of personal data and other confidential information) are in place.

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 controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Any such request does not require that an official School form be filled in, nor need it refer to the correct legislation, an individual must only ask that they would like access to the personal data the School holds on them. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Bursar and the Compliance Officer immediately.

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; and
- 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.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

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 Compliance Officer and the Bursar immediately.

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. See Data Handling and Individual Responsibilities above.

Sharing Personal Data and information security

The School will generally not share Personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the Personal Data complies with the privacy notice that has been provided to the Data Subject and, if required, the Data Subject's consent has been obtained or there is another legal basis on which to share the Personal Data;

- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the police, the Local Authority, the Independent Schools Inspectorate (ISI) or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The School will take reasonable steps to make the disclosure secure, including verifying the identity of the third party.

If a staff member is uncertain about whether or not they should share data, or if they are being asked to share data in a new way, they should speak to the Compliance Officer. Before sharing personal data, staff should:

- make sure they are allowed to share it;
- ensure adequate security;
- ensure that any emails which contain sensitive personal data are encrypted;
- if asked to disclose information to the Police speak to the Compliance Officer or Bursar and ensure the request is made in writing;
- if asked to disclose personal data to a contractor or to an individual where they are unsure of identity (e.g. if a request has come from a parent using a different or non- registered email address) they should check with the Bursar or the Compliance Officer.

Guidance will be provided in reference to the ICO Data Sharing Checklist

Information security is important, and all staff should seek to ensure that security breaches do not occur. Examples in a school environment could be using a mobile phone which is not password protected, sending personal data or special category personal data to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Staff must do all they can to ensure that personal data is not lost, or damaged, or accessed, or used without proper authority.

Staff should:

- be careful when sending correspondence containing personal data and/or special category data. Staff should check email addresses and if in doubt send a ‘test’ email. Extreme care must be taken when attaching files to emails;
- be careful when sharing documents in Heritage Google Drive;
- do not use or leave computers, devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons;
- be vigilant of the risks of others viewing confidential documents. Paper documents should be locked away when not in use and carried in envelopes/folders;
- use bcc (blind carbon copy) where appropriate;
- lock computers when not in use;
- keep passwords secure and only use your Heritage password for your Heritage account;
- use encryption where handling personal or confidential data;

Processing of Financial Data

The School carefully handles financial information including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details), may not be

treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

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 to be used like this?
- 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. Rather it should be viewed as a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture, and all our staff and representatives must be mindful of it.

Authorised by	Jason Fletcher
Date	December 2025

Review date	December 2026
Circulation	Staff and parents via website

Appendix 1 - Legal basis for processing information

The School must only collect, process and share Personal Data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing Personal Data and Special Category Data as set out in the UK GDPR.

Before processing starts for the first time, the Schools will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing.

Personal Data Processing Conditions	**Special Category Data Processing Conditions**
The Data Subject has given their consent	The Data Subject has given their explicit consent
The processing is necessary for the performance of a contract with the Data Subject or for taking steps at their request to enter into a contract	The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Schools in the field of employment law, social security law or social protection law
To protect the Data Subject's vital interests	To protect the Data Subject's vital interests
To ensure the School's comply with laws and regulations (other than contractual obligations)	The processing is necessary for the establishment, exercise or defence or legal claims or whenever courts are acting in their judicial capacity
To perform a task in the public interest or in order to carry out official functions as authorised by law	To perform a task in the substantial public interest or in order to carry out official functions as authorised by law
For the purposes of the Schools' legitimate interests where authorised and in accordance with, data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the Data Subject.	Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
	Where it is necessary for reasons of public interest in the area of public health
	The processing is necessary for archiving, statistical or research purposes
	Where the data has been made public by the Data Subject