HEATHFIELD SCHOOL

Data Protection Policy

Policy Area:	General
Relevant Statutory Regulations:	ISSR Part 3 Data Protection Act 2018 Protection of Freedoms Act 2012 Education Pupil (Information) Regulations 2005 The Privacy and Electronic Communications Regulations 2011
Key Contact Personnel in School	
Nominated Member of Leadership Staff Responsible for the policy:	Manager of IT Services and Network and Bursar
Version:	202.01
Date updated:	01 February 2021
Date of next review:	01 February 2024

This policy will be reviewed at least triannually, and/or following any concerns and/or updates to national and local guidance or procedures.

Introduction

Heathfield School ("the School") is required to process relevant personal data regarding staff, pupils and their parents and guardians, as part of its operation and shall take all reasonable steps to do so in accordance with the Data Protection Act 2018, and this Data Protection Policy (the "Policy").

Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy any reference to staff or pupils includes current, past or prospective staff or pupils.

The purpose of this Policy is to show how the School deals with personal information so as to ensure that it does so correctly and securely and in accordance with the General Data Protection Regulations and other related legislation. This Policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All staff and Governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this Policy.

Background

Data protection is an important legal compliance issue for the 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, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as "data controller", is liable for the actions of its staff and Governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring the School complies with and is mindful of the School's legal obligations, whether that personal data handling is sensitive or routine.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act 2018 (DPA) was also passed to deal with certain issues left for national law. The DPA included 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.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has 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, 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:

- **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 by its Governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data 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. That is not simply a name but any 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. This personal data may include (but is not limited to): names and addresses, bank details, academic, disciplinary, admissions and attendance records, references, examination scripts and marks. CCTV Video is also captured and recorded in order to maintain the security of the premises. It makes no difference if the individual can be identified directly from the record itself or indirectly using other information in the School's possession or likely to come into the School's possession.
- **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.

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 parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or Governors 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 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 "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – 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 School has appointed the Manager of IT Services and Network as Privacy Officer (PO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the General Data Protection Regulations (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 Privacy Officer.

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 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); 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 Data Protection Act 2018 (DPA) 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 DPA (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 Notices, as 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.

Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding a member of staff, a pupil and their parents or guardian. Sensitive personal data includes information about a person's mental or physical health or condition and data relating to religion, race, ethnicity, sexual life or orientation, trade union membership, political views or criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will be required in writing except in extreme circumstances (having taken professional advice) where the welfare and safety of the pupil is at risk.

Privacy Notice

Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or statement.

The privacy notice is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 1231113 or at: https://ico.org.uk/concerns/.

Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided. Copies of the School's privacy notices for pupils, staff, visitors and parents can be obtained from the Privacy Officer and are available on Teams.

Having said this, staff should inform the Privacy Officer if they suspect that the School is using personal data in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the School is collecting medical information about pupils without telling their parents what that information will be used for.

Access to Data

Individuals have a right of access to information held by the School. A request for data held by the School about the individual making the request is termed a Subject Access Request (SAR). Any reasonable request by a pupil (if deemed to be of an age and understanding that they can make such a request), parent or member of staff wishing to access their personal data should put their request to the PO. SAR can be made verbally but the School will ask individuals to confirm their request in writing, to enable clarity on the scope of any request and the timescale for a response. It does not follow that, just because a child has the capacity to make a SAR, they also have capacity to consent to sharing their personal data with others, as they may still not fully understand the implications of doing so. This should be reviewed on a case-by-case basis. Parent's making a SAR on behalf of a child should be advised that the child may be deemed to be of an age and understanding whereby consent should be sought. If so, the consent and express permission of the child will be sought prior to any release of data. Express permission should be in the form of a signed consent form. The School will endeavour to respond to any such requests as soon as is reasonably practicable and in any event, within 30 days for access to personal records.

If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Privacy Officer as soon as possible.

Appendix 1 provides further details regarding Subject Access Requests.

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.

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 some instances the School may refuse access. This may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil's examination scripts, employment references made by the School which remain in the control of the School, or planning information relating to staff, if it may be deemed to damage School business to disclose it.

Whose Rights?

The rights under the DPA are the individual's to whom the data relates. The School will, however, in most cases rely on parental consent to process data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is unreasonable in all the circumstances to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted.
The School will only grant the pupil direct access to her personal data if, in the School's reasonable belief, the pupil understands the nature of the request. Pupils agree that the School may disclose their personal data to their parents or guardian.

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds her agreement to her personal data being disclosed to her parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding her consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Exemptions

Certain data is exempt from the provisions of the DPA which includes the following:

- the prevention or detection of crime
- all Safeguarding matters take precedent over data privacy, for instance the provision of staff or pupil information to the LEA or the Police
- the assessment of any tax or duty
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School

The above are examples only of some of the exemptions under the DPA. Any further information on exemptions should be sought from the PO.

Disclosure of Information

The School may receive requests from third parties to disclose personal data it holds about staff, pupils, their parents or guardians. The School confirms that it will not (except in specific circumstances, having taken professional advice) disclose information unless the individual has given their consent or one of the specific exemptions under GDPR applies. However the School does intend to disclose such data as is necessary to third parties for the following purposes:

- to give a confidential reference relating to a member of staff for employment elsewhere or for a disciplinary reason or in the case of a pupil to any educational institution which it is proposed that the pupil may attend
- to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend
- to publish the results of public examinations or other achievements of pupils of the School
- to disclose details of a member of staff's or pupil's medical condition where it is in that person's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

Use of Personal Information by the School

The School will, from time to time, make use of personal data relating to pupils, their parents or guardians in the following way. Parents/Guardians and pupils over the age of 18 will be requested to give their express permission for the School to use photographic and video images of the pupils. A consent form is issued upon acceptance of a place which should be read, signed and returned to the Registrar. Should you wish to limit or object to any such use please notify the PO and Director of Marketing and Admissions in writing.

1. To make use of photographic images of pupils in School publications, School social media platforms and on the School website. However, the School will not publish photographs of individual pupils with their surnames on the School website or social media platforms without the express agreement of the appropriate individual.
2. For fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, including transferring information to any association, society or club set up for the purpose of establishing or maintaining contact with pupils or for fundraising, marketing or promotional purposes.
3. To include pupils in promotional School videos for use on the School website and School social media platforms.

Accuracy

The School will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the PO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Care and Data Security

The School will take reasonable steps to ensure that members of staff will only have access to personal data relating to staff, pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the DPA. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons.

The School will 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. This is in relation to data belonging to both staff and pupils. Staff should not remove personal data from the School's premises unless it is stored on a password protected computer or encrypted memory device.

Paper records which include confidential information shall be kept in a cabinet and/or office which is kept locked when unattended. All paper records should be kept in a secure location. Paper records that include safeguarding, child protection and sensitive information relating to safeguarding are kept in a locked cabinet in a locked office.

The School uses an array of measures to protect personal data stored on computers, and internal IT systems including file encryption, anti-virus and security software, user passwords, audit trails and backup systems. Staff must keep any passwords secure. Staff should be mindful that passwords are not always effective and are not a substitute for encryption.

Use of personal email accounts or unencrypted personal devices by Governors or staff for official School business is not permitted.

No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.

More generally, the School requires all staff (and expect all our contractors) to remain mindful of the data protection principles, 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. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

The School expects 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 Privacy Officer, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

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 in this policy, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files 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 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 staff handbook 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 related policies listed at the end of this document.

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.

References

References given by any member of School staff, whether for staff or pupils, may be given only with the consent of the Headmistress or Bursar unless the reference is written by the Headmistress or Bursar or Deputy Bursar, in consultation with other staff where appropriate. Any reference will be fair, balanced, reasonable and will be provided in good faith. All references for staff must be forwarded to the Deputy Bursar prior to being issued externally to ensure factually correct.

A request for a reference to be provided to an employer or institution overseas will be taken as the applicant's confirmation that the receiving country ensures an adequate level of protection for the rights and freedoms of *data subjects*.

In exceptional circumstances the Headmistress may agree to provide a written testimonial. It should be noted that this does not constitute a reference or an open reference.

Under the Data Protection Act 1998, references given by an organisation were exempt from disclosure on receipt of a SAR. The exemption only applied to references given by the organisation. This meant that the exemption could only be used by the provider of the reference, and not a recipient.

Under the Data Protection Act 2018 this distinction was removed so that any reference provided in confidence is exempt from disclosure under a SAR. This means that if the School receives a subject access request, confidential employment references about the individual making the request, whether created by the School or received from a third party, will be exempt from disclosure.

Timely Processing

The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

Enforcement

If an individual (other than a staff member) believes that the School has not complied with this Policy or acted otherwise than in accordance with the GDPR, they should utilise the School Complaints Procedure and should also notify the PO. If the individual is a staff member they should utilise the School Grievance Procedure.

Data Breaches

One of the key new obligations contained in the DPA is on reporting personal data breaches.

Any actual data breach or alleged data breach must be reported to the Privacy Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the School becomes aware of a significant data breach as determined by the Privacy Officer it has 72 hours in which to report the breach to the Information Commissioner's Office. Examples of breaches and their seriousness for reporting purposes are:

- mistakenly sending an email containing personal data to an incorrect recipient.
- theft of IT equipment containing personal data.
- failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Privacy Officer.

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 already stated, 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.

Processing of Financial Data

Some categories of 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.

Further Information

The School has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.org.uk under registration number Z5785153. This website also contains further information about data protection.

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.

Related Policies

- CCTV Policy
- Complaints Policy
- Confidentiality Policy
- IT Acceptable Use Policy
- Privacy Notice for COVID 19 Testing Policy
- Privacy Notice for Enquiries Policy
- Privacy Notice for Parents Policy
- Privacy Notice for Pupils Policy
- Privacy Notice for the School Workforce Policy
- Privacy Notice for Visitors Policy
- Record keeping Policy
- Safeguarding Children and Child Protection Policy
- Taking, Storing and Using Images of Pupils Policy

Appendix 1 - Dealing with a subject access request

Requests for information can be made verbally but should be followed up in writing (which includes the use of e-mail). If the initial request does not clearly specify the information required, then the School will make further enquiries.

The PO must be confident of the identity of the individual making the request. When the request concerns data about a pupil, checks will also be carried out regarding proof of relationship to the child. In addition, evidence of identity will be established by requesting production of:

- Passport
- Driving licence
- Utility bills with the current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement (this list is not exhaustive)

As stated above, any individual has the right of access to information held about them. However, in the case of children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The PO should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.

The response time for subject access requests, other than for educational records, is 30 days from receipt (this refers to calendar days irrespective of school holiday periods).

DPA allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

Third party information is information that has been provided by another person such as the local authority, the police, a health care professional or another school. It is normal good practice to seek the consent of the third party before disclosing information. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed. (There is no need in the case of third party requests to adhere to the 30 day statutory timescale.)

Any information that could cause serious harm to the physical, emotional or mental health of a pupil or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.

If there are concerns about the disclosure of information, then additional advice should be sought, usually from the Information Commission's Office.

When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.

Information can be provided at the School with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when

considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.

Complaints will be dealt with in accordance with the School complaints procedure, which is available on-line. Should the complainant wish to take the matter further, it may be referred to the Information Commissioner www.ico.org.uk.

Appendix 2 – Data Expiry

In accordance with Data Protection and the GDPR, Heathfield School complies with good data cleaning practice. The School's policy on data deletion is as follows:

E-Mail
An automated retention policy applies to all mailboxes. This policy retains messages as follows, with all expired messages being deleted nightly by the system:

- Inbox 1 year
- Sent items 2 years
- Personal folders 7 years

Files & Documents
All files and documents held in any cloud storage systems are kept for a maximum period of 10 years since the file was last modified.

Management Information Systems
Student records are deleted after 7 years from the date of the student leaving, or when the student reaches the age of 25. Staff records are deleted after 7 years from the date of their leaving.

Donor Strategy Old Girls (Fellowship) Database
Fellowship data is kept in perpetuity but anyone retains the right to be forgotten, upon which request received in writing their data will be deleted.

Backups
All backups of essential data are kept for a maximum period of 7 years from the date of backup. If the backups live on cloud storage, the files are deleted. If the backups live on physical media such as DVDs, Blu-Ray discs or hard disk drives, the physical media is destroyed to make retrieval of the data impossible.

Please note that Safeguarding matters override Data Protection and, in serious cases, data will be retained in perpetuity.