TORMEAD

POLICY FOR THE PROCESSING, STORAGE, RETENTION, ARCHIVING & DESTRUCTION OF PERSONAL DATA

1. EMPLOYEES

1.1 Purpose of this Policy

The General Data Protection Regulation ('GDPR') (effective across the UK from 25 May 2018) impose stricter rules regarding the storage and use of personal data, with the practical effect of requiring more dynamic, efficient and secure storage systems such that:

- All information held by School needs to be justifiable, by reference to its purpose;
- The School must be transparent and accountable as to what it holds, and understand why it holds it;
- Schools must be prepared to respond quickly to subject access requests;
- Personal data collected should be auditable as far as possible; and
- Personal data must be held securely and accessed only by those with reason to view it.

The School processes the personal data, including special category personal data, of its employees in accordance with the School's Privacy Notice; the purpose of this section of this Policy is to document how we process, store, retain, archive and destroy employee personal data. The School has completed a data audit which has, inter alia, identified the legal bases on which the School processes employee personal data, to include:

- compliance with legal / statutory obligations;
- for performance of the employment contract; and
- for legitimate business interests.

1.2 Which employee personal data does this Policy apply to?

For the purposes of this Policy, we use the term 'employee personal data' to refer to the personal data of all individuals who are included on the School's Single Central Register ('SCR') - namely:

- All paid employees;
- Governors;
- Volunteers; and
- Peripatetic teachers and coaches.

1.3 What type or records and documents does this Policy apply to?

Records means any document or item of data that includes the personal data of an employee, and includes both digital and paper records.

The School processes a wide range of employee personal data. Some personal data, such as NI number, bank account details, payroll information and pension records, are processed to discharge the obligations of the employment contract between the School and the

employee. Other personal data, such as confirmation of identity, health information and references, are processed to comply with our statutory obligations.

In addition to the personal data described above which is provided by the employee to the School, typically during the recruitment process, further personal data may be generated during the course of employment to include:

- Minutes of meetings in which staff matters were discussed;
- Email correspondence on staff matters;
- Records of disciplinary or capability matters;
- Sickness absence records; and
- CCTV images.

1.4 How do we store employee personal data?

Every current employee has an individual paper based file. These files are stored in secure cabinets in a locked room accessible only by the Headmistress, the Bursar, & the HR & Payroll Officer. The Estates & Facilities Manager and the Premises team can also access this room in the event of an emergency.

The individual paper based files of former employees are retained and then destroyed as set out in section 7 of this Policy. Whilst a full paper based file is in existence for a former employee, it is stored in a secure, locked cabinet in the HR & Payroll Officer's room; only the Bursar & the HR & Payroll Officer have keeps to this cabinet.

Electronic employee data is filed in the 'Bursar & HR' folder on the School's secure onsite network. The Bursar & HR folder contains individual electronic employee files for a number of employees which contain similar information to that found in the paper based individual employee file; only employees employed since September 2012, or whose role has changed since that date, have such an electronic file.

The SCR is saved on the School network, as are electronic files of monthly payroll. Only the Bursar, the HR & Payroll Officer and IT services have access to the 'Bursar & HR' folder

Microsoft Office is hosted on the School's server, as is ISAMS. Minutes of meetings, which may contain employee personal data if staff matters are discussed, are stored on the School network or on OneDrive.

Employee performance appraisal paper documents are filed in employee personnel files.

Employee data stored in ISAMS is only accessible by the Executive Group, IT staff, Medical staff, Office staff, the Registrar and the cover supervisor.

Training records, including Child Protection Training records, are stored on the School network or OneDrive.

It is the School's policy that important documents and sensitive / special category personal data should not be taken home by any staff member. This includes it being kept or carried on a portable device (CDs, data sticks, mobiles and electronic tablets) unless it is absolutely necessary, in which case it should be subject to a risk assessment.

1.5 Do we share any employee personal data with third parties?

Elements of payroll are outsourced to Smith & Williamson and employee personal data therefore passes between the School and Smith & Williamson on a monthly basis. Data is transferred by email and all files are password protected; the password is known only to the Bursar, the HR & Payroll Office and the Smith & Williamson payroll team.

Pension information is submitted monthly to the Teachers' Pension Scheme and, in respect of support staff who are members of the defined contributions scheme, to the Pensions Trust. The web-based portals of both scheme contain employee personal data; both require a User ID and password, which are known only to the Bursar & the HR & Payroll Officer.

We use Atlantic Data to process DBS checks and the Atlantic Data portal retains historical applications; our policy is to delete DBS details from the portal after six months.

No employee personal data is transferred outside the UK.

1.6 Are employees aware of the personal data we process and hold?

The School's Privacy Notice is published on our website. In addition:

- New members of staff are provided with a copy of the Privacy Notice and both individual employment contracts and the employment manual contain clauses and sections which reinforce the information in the Privacy Notice
- Other 'employees' who are not subject to an employment agreement with the School (for example, Governors and volunteers) are provided with a copy of the Privacy Notice on commencement of their service
- The School's standard application form includes a hyperlink to the Privacy Notice on the website and also provides candidates with a summary of how we process the CVs and other information they may submit, and how long we retain them for (with an opt-out option)

1.7 How do we retain, archive and destroy employee personal data?

The paper-based and electronic individual employee files are **retained in their entirety for 7 years** after the employee leaves. After 7 years, paper files are securely destroyed and electronic files are deleted, save that the School retains a record of the following information, for reference purposes, on a spreadsheet:

- Name
- Job title
- Dates of employment
- Final salary

Accident report forms for staff are held by the Estates & Facilities Manager in hard copy for a minimum of four years and are reviewed on a case by case basis as required. The file is kept in a locked cupboard only accessible by the Estates & Facilities Manager.

Any information relating to a Safeguarding matter is stored separately by the Headmistress and is retained indefinitely.

Upon leaving, an employee is transferred to the leavers' section of the SCR and this spreadsheet is also retained indefinitely (as previously, this document is stored on Torfiles with access restricted to the Bursar and the HR & Payroll Officer).

Payroll information is retained in its entirety for 7 years; after 7 years, paper copies are securely destroyed and electronic files are deleted, save for pension reports which are retained indefinitely.

On the date an employee leaves the School, their profile is permanently deleted from ISAMS.

The School's policy is that all emails are deleted after a period of 3 years.

During the recruitment process we receive CVs, application forms and equal opportunity monitoring forms. Some candidates are interviewed, generating interview notes; candidates also bring ID documents to their interview. We destroy the ID documents of the unsuccessful candidates immediately after the appointment of the successful candidate. We file in a locked cupboard in the HR & Payroll Officers' office all the other details for six months for the purpose of responding to potential employment tribunal claims arising out of the recruitment process. **After six months the documents are securely destroyed, unless a candidate has opted-in to the longer (12 months) retention of their personal data in connection with potential future opportunities that may arise.**

DBS certificates are retained for 6 months, at the maximum, and are then securely destroyed.

The Equal Opportunities Monitoring Form is filed separately from the application form and is not used in the recruitment decision making process. Six months after appointment, the data is processed and the forms are destroyed. The processed data does not include any personal data.

Documents that require secure destruction are either shredded in our onsite machine or disposed of in one of four confidential waste bins. We have a 3 year contract with Restore Data Shredding that expires March 2020. Twelve collections are scheduled over twelve months. The confidential waste is then destroyed off site, at one of Restore Data's depots.

2. CURRENT AND PAST PUPILS, AND THEIR PARENTS, CARERS OR GUARDIANS

2.1 Purpose of this Policy

The General Data Protection Regulation ('GDPR') (effective across the UK from 25 May 2018) impose stricter rules regarding the storage and use of personal data, with the practical effect of requiring more dynamic, efficient and secure storage systems such that:

- All information held by School needs to be justifiable, by reference to its purpose;
- The School must be transparent and accountable as to what it holds, and understand why it holds it;
- Schools must be prepared to respond quickly to subject access requests;
- Personal data collected should be auditable as far as possible; and
- Personal data must be held securely and accessed only by those with reason to view it.

The School processes the personal data, including special category personal data, of its current and past pupils and their parents, carers or guardians in accordance with the School's Privacy Notice; the purpose of this section of this Policy is to document how we process, store, retain, archive and destroy this personal data. The School has completed a data audit which has, inter alia, identified the legal bases on which the School processes pupil and parent personal data, to include:

- compliance with legal / statutory obligations;
- for performance of the parent contract; and
- for legitimate business interests.

2.2 Which pupil and parent personal data does this Policy apply to?

For the purposes of this Policy, we use the term 'pupil personal data' to refer to the personal data of all individuals who are, or have been, included on the School's Admissions Register along with their parents, carers or guardians.

2.3 What type or records and documents does this Policy apply to?

Records means any document or item of data that includes the personal data of a current or past pupil, parent, carer or guardian, and includes both digital and paper records.

The School processes a wide range of pupil personal data, the majority of which is processed to comply with our statutory obligations.

In addition to the personal data described above which is provided by the parent to the School, typically during the admissions process, further personal data may be generated during the course of a pupil's School career to include:

- Email correspondence on pupil matters;
- Records of pertinent conversations between staff and pupils and/ or parents, carers or guardians;
- Medical records;
- Child protection files;
- Learning support records;
- Examination results;
- Minutes of meetings in which pupil performance was discussed;
- Academic tracking and monitoring data; and
- CCTV images.

2.4 How do we store pupil personal data?

2.4.1 Every current pupil has an individual paper-based file. These files are stored in locked cabinets in the Senior School Office (girls in Years 7 - Upper Sixth) and the Junior School meeting room (girls in Reception - Year 6) and are accessible by all current Tormead staff. They contain all forms, reports and references pertaining to the admissions process, as well as any correspondence sent or received by School during the course of a girl's career.

2.4.2 Every current pupil also has an individual electronic entry on ISAMS, our Information Management System, which is accessible to all current Tormead staff with a log-in and password. This contains similar information to that found in the paper based individual pupil file as well as an individual photograph, attendance records, medical records and academic assessment data including half-termly grades and annual reports.

2.4.3 Records of pertinent conversations between staff and pupils and/ or parents, carers or guardians are stored securely under each girl's name on OneDrive. In the Senior School, these are accessible by the Executive Group, Heads of Year, Wellbeing Centre and Senior School Office staff. In the Junior School, these are accessible by the Junior School Senior Team and Junior School Office staff. A summary document of daily incidents (Daily Record)

pertaining to girls is shared amongst all teaching staff daily via an email link to a PDF, with the Junior and Senior Schools producing their own versions. Records which pre-date digital storage may be found in hard copy on a pupil's paper-based file.

2.4.4 Medical information supplied by parents during the admission process, as well as via yearly update forms, is held on a pupil's individual paper-based file. It is also stored on ISAMS. Paper-based medical records (e.g. historic daily logbooks, immunisation lists) are kept in a locked filing cabinet in the Medical Centre accessible by Wellbeing Centre staff. Counselling notes are kept, with names coded as letters and numbers, in a locked cupboard in the Counselling Room which is itself kept locked and is only accessible to the Counsellor.

Accident report forms for pupils are held by the Estates & Facilities Manager in hard copy for a minimum of four years and are reviewed on a case by case basis as required. The file is kept in a locked cupboard only accessible by the Estates & Facilities Manager.

2.4.5 Individual paper-based child protection files are stored in a locked cabinet in the Headmistress' Study. The chronological record book for all child protection cases is stored in a locked cabinet in the Deputy Headmistress' office. In the event of an emergency, the Headmistress or Deputy Headmistress can each access the child protection files held by the other. The sanctions, restraint and bullying logs are stored in a locked filing cabinet in the Deputy Headmistress' office.

2.4.6 Electronic learning support records for individual girls are stored securely on OneDrive and are accessible by the Head of Learning Support and members of her department. Paper-based learning support records for individual girls are stored in a locked filing cabinet in the Head of Learning Support's Office. Selected learning support information, including the current register, IEPs and LUCID scores is shared with all teaching staff via OneDrive. Learning support access arrangement evidence and Form 8 documents are held by the Examinations Officer as outlined in 2.4.7 below.

2.4.7 Individual girls' examination results are stored in the locked Examinations Office. Paper-based files which evidence medical issues relating to examination access arrangements as well as those which evidence access arrangements, along with original Form 8 documents, are kept in filing cabinets in the locked Examinations Office. The Examinations Office is only accessible by the Examinations Officer and the Headmistress.

2.4.8 Information pertaining to the administration of teaching and learning is stored on OneDrive; this includes but is not limited to, academic tracking and monitoring information and the minutes of meetings in which girls' progress is discussed. Paper-based documents may also be used for this purpose. Individual teachers maintain mark books which list girls' names; these may be hard copy or digital.

MIDYIS and ALIS scores as well as pupil performance management data are kept on the School network.

2.4.9 Data relating to educational visits is stored in hard copy in a filing cabinet in the relevant School Office until the end of the term in which the visit took place. It is then edited to include:

- final details form
- risk assessment
- list of girls attending

These edited documents are then saved in the 'Visits Archive' folder on OneDrive. All other information relating to the visit (e.g. medical information, passport copies, letters and sign-up forms etc) is securely destroyed.

The edited documents are stored in the archive for one year, after which point they are deleted.

2.4.10 Parents' bank account details are stored on the PASS system, accessible only by the Bursar, the Accounts team and IT. Paper-based bursary records are stored in the Bursar's Office whilst the recipient of the bursary attends the School.

2.4.11 Biometric data is collected from Sixth Form girls in order to facilitate registration. It is limited to fingerprint data and both girls' and parents' consent is sought. This data is stored securely on the School server. Please refer to the School's Biometric Data Policy for further details.

2.4.12 CCTV images may be captured for security purposes. They are stored on tape for a maximum of 28 days, after which they are overwritten. Please refer to the School's CCTV Policy for further details.

It is the School's policy that important documents and sensitive / special category personal data should not be taken home by any staff member. This includes it being kept or carried on a portable device (CDs, data sticks, mobiles and electronic tablets) unless it is absolutely necessary, in which case it should be subject to a risk assessment.

2.5 Do we share any pupil or parent personal data with third parties?

In line with our statutory obligations, we share information relating to child protection records with other Schools and with external agencies, as appropriate; hard copies are sent via registered post, with proof of receipt required, and copies of files kept as outlined in 2.4.5 above. Any email correspondence is sent using the Egress encryption system. We are required to inform the Surrey County Council of all pupil leavers and joiners under statutory school age; this is sent to a secure email address which uses encryption.

Learning support information is shared with examination boards in the event of a special access arrangements request or occasionally with external assessment centres. In both cases, girls and parents are asked to sign to give their consent to this. Copies of Form 8 documents may also be shared with other Schools if requested after a girl transfers, with girls and parents asked to sign to give their consent.

Girls' names are shared with the University of Durham's CEM in order to create data for tracking academic performance.

Occasionally, employers request confirmation of individuals' public examination results. In these instances, we share this data once we receive confirmation from the individual that they consent.

We share references for our pupils with other Schools once email consent from parents has been received by the Headmistress.

Parents' contact and bank account details are inspected annually by auditors. WCBS (who provide and support PASS) can also access our system (and therefore data) remotely. Parents' bank account details are shared with Lloyds and submitted via Bottomline Technologies.

No pupil or parent personal data is transferred outside the UK.

2.6 Are pupils and parents aware of the personal data we process and hold?

The School's Privacy Notice is published on our website. In addition:

- New parents are provided with a copy of the Privacy Notice appended to the Terms & Conditions
- Existing parents are sent an annual reminder of the Privacy Notice's existence and directed where they can find it on the website
- Girls are sent an annual reminder of the Privacy Notice's existence.

2.7 How do we retain, archive and destroy pupil and parent personal data?

2.7.1 Paper-based individual pupil files are edited after a girl leaves the School, with all information removed securely destroyed; the information retained includes:

- application form
- registration form
- signed contract
- offer letter
- exam scripts
- references from previous Schools
- records of pertinent conversations

These files are then stored in the School's secure storage facility until the girl to whom they pertain reaches the age of 25, at which point they will be securely destroyed.

2.7.2 An individual girl's electronic entry on ISAMS will be edited to include:

- name, date of birth and contact details (address and email)
- attendance record
- medical record
- grades and reports
- public examination results
- membership of TOGA alumnae association

When the girl reaches the age of 25, it will be edited further to include:

- name, date of birth and contact details
- dates of attendance
- membership of TOGA alumnae association

This record will then be stored on ISAMS indefinitely.

2.7.3 Records of pertinent conversations between staff and pupils and/ or parents, carers or guardians are archived into a folder on OneDrive when a girl leaves the School and stored until she reaches the age of 25, at which point they will be deleted. PDF copies of the Daily Record are kept for a maximum of one week before being deleted, thus rendering the email link inoperative.

2.7.4 Medical information supplied by parents during the admission process, as well as via yearly update forms, is dealt with as outlined in 2.7.1 and 2.7.2 above.

Paper-based medical records (e.g. historic daily logbooks, immunisation lists) are kept in a locked filing cabinet in the Medical Centre accessible by Wellbeing Centre staff for a minimum of seven years, after which point they will be securely destroyed. Paper-based counselling notes are kept, with names coded as letters and numbers, in a locked cupboard in the Counselling Room which is itself kept locked and is only accessible to the Counsellor. These are stored until the girls to whom they pertain reach the age of 25, after which they are securely destroyed.

Accident report forms for pupils are held by the Estates & Facilities Manager in hard copy and will be reviewed on a case by case basis as required. The file is kept in a locked cupboard only accessible by the Estates & Facilities Manager. These forms are stored until the girl reaches the age of 25, at which point they are securely destroyed.

2.7.5 Individual paper-based child protection files, along with the chronological record book of child protection cases, are stored as outlined in 2.4.5 above and kept indefinitely.

NB It should be noted that, in line with local safeguarding board advice in place up to May 2018, previous practice was to shred child protection files when a girl reached the age of 25 or, in the case of girls transferring to other Schools, to shred the copy of the file when acknowledgement of file receipt was received. As such, there is not a comprehensive record on file.

Records of girls' names in the sanctions and restraint logs are kept until the girl reaches the age of 25, at which point her name is redacted. Those in the bullying log are kept indefinitely, in line with arrangements for child protection documentation.

2.7.6 Electronic learning support records for individual girls are archived into a folder on OneDrive when a girl leaves the School and stored until she reaches the age of 35, at which point they are deleted. Paper-based learning support records for individual girls are stored in a locked filing cabinet in the Head of Learning Support's office; these will be securely destroyed when the girls to whom they pertain reach the age of 35. Selected learning support information pertaining to leavers which is shared with all staff will be archived on a girl's individual record and stored as above (IEPs) or deleted (current register, LUCID scores) as appropriate. Learning support access arrangement evidence and Form 8 documents are held by the Examinations Officer as outlined in 2.7.7 below.

2.7.7 Paper-based records of individual girls' examination results are stored in the locked Examinations Office. When the girl reaches the age of 25, these are securely destroyed. The Examinations Officer also maintains a record of the examination boards and subjects taken each year to facilitate future individual results enquiries. Paper-based files which evidence medical issues relating to examination access arrangements are kept in filing cabinets in the locked Examinations Office and securely destroyed after the deadline for results enquiries in the year in which the examinations were taken. Paper-based files which evidence access arrangements, as well as original Form 8 documents, are kept in filing cabinets in the locked Examinations Office and securely destroyed when the girl reaches the age of 35. The Examinations Office is only accessible by the Examinations Officer and the Headmistress.

2.7.8 Information pertaining to the administration of teaching and learning is stored on OneDrive for up to three years. At the end of each academic year, staff delete all electronic documents and/ or securely destroy all paper-based documents pertaining to the academic year which ended three years before. This includes, but is not limited to, academic tracking and monitoring information, minutes of meetings in which girls' progress is discussed, and markbooks.

MIDYIS and ALIS scores as well as pupil performance management data are kept on the School network until the girls to whom the data pertain reach the age of 25, at which point they are deleted.

Departments may, of course, choose to keep anonymised data in order to use it for the purposes of statistical analysis.

2.7.9 Data relating to educational visits is stored in hard copy in a filing cabinet in the relevant School Office until the end of the term in which the visit took place. It is then edited to include:

- final details form
- risk assessment
- list of girls attending

These edited documents are then saved in the 'Visits Archive' folder on OneDrive. All other information relating to the visit (e.g. medical information, passport copies, letters and sign-up forms etc) is securely destroyed at this point.

The edited documents are stored in the archive for one year, after which point they are deleted.

2.7.10 Parents' bank account details are stored on the PASS system. Paper-based bursary records are stored in the Bursar's Office and securely destroyed upon the conclusion of the audit of the subsequent year to that to which they relate.

2.7.11 Biometric data are collected from Sixth Form girls in order to facilitate registration. It is limited to fingerprint data and both girls' and parents' consent is sought. This data is stored securely on the School server and deleted as soon as the girl leaves the School. Please refer to the School's Biometric Data Policy for further details.

2.7.12 CCTV images may be captured for security purposes. They are stored on tape for a maximum of 28 days, after which they are overwritten. Please refer to the School's CCTV Policy for further details.

The School's policy is that all emails are deleted after a period of 3 years.

3. PROSPECTIVE PUPILS, AND THEIR PARENTS, CARERS OR GUARDIANS

3.1 Which Admissions personal data does this Policy apply to?

The General Data Protection Regulation ('GDPR') (effective across the UK from 25 May 2018) impose stricter rules regarding the storage and use of personal data, with the practical effect of requiring more dynamic, efficient and secure storage systems such that:

- All information held by School needs to be justifiable, by reference to its purpose;
- The School must be transparent and accountable as to what it holds, and understand why it holds it;
- Schools must be prepared to respond quickly to subject access requests;
- Admissions data collected should be auditable as far as possible; and
- Admissions data must be held securely and accessed only by those with reason to view it.

The School processes Admissions data in accordance with the school's Privacy Notice; the purpose of this Policy is to document how we process, store, retain, archive and destroy this data. The School has completed a data audit which has, inter alia, identified the legal bases on which the School processes Admissions data, to include compliance with legal / statutory obligations and legitimate business interests.

3.2 Which Admissions personal data does this Policy apply to?

For the purposes of this Policy, we use the term 'Admissions data' to refer to the personal data of all prospective parents and pupils who either make an enquiry about applying to Tormead or who submit a completed Registration Form at the start of the Admissions Process. It also refers to all of the specific information collated to support a candidate's admission into the School.

3.3 What type or records and documents does this Policy apply to?

Records means any document or item of data that includes the personal data of a prospective parent or pupil, and includes both digital and paper records.

We collect a range of personal data to support the Admissions process via enquiry forms on the School Website and / or the Registration Form and via email enquiries, completed examination entry forms and scholarship entry forms. This includes address and other contact details for the candidates and their parents, the candidate's date of birth, and the candidate's schooling history. Additional data is collected during the Admissions Process to include academic references from a girl's current school, education psychologist reports, and completed examination papers. This data is used to contact the prospective parents throughout the Admissions Process and to assist in decisions about offering School places. Additionally, completed Acceptance forms received from parents are retained as proof of contractual relationships established between the Parents and the School if a place at Tormead is formally accepted.

In addition to the personal data described above further personal data may be generated during the course of Admissions process to include, but not restricted to:

- postal correspondence detailing the Admissions process, inviting individuals to an event, or notifying candidates of examination outcome;
- email correspondence;
- spreadsheets or word documents tracking attendance at events; and
- spreadsheets reporting examination results.

3.4 How do we store Admissions data?

The RS database serves as the system of record for the Admissions data and is used to track individuals through the Admissions process from their initial enquiry right through to the point when decisions are taken about offering places and accepted or declining these places. RS is a confidential database hosted by Tormead. The information it contains is accessed only by the Admissions Team and, where necessary for support purposes, the IT Team.

In addition to the information held in RS, paper files are created for each registered candidate. These files contain the registration forms, postal correspondence and other paper based records required to support the application process. This includes, but is not limited to, academic references received from other Schools, education psychologist reports, completed examination papers, and acceptance forms. These files are retained in locked filing cabinets in the Admissions Office and are only accessed by the Admissions Team and members of staff directly involved in the entry assessment process.

All other electronic documents, including Word Documents and spreadsheets, generated by the Admissions Team as part of the Admissions Process are retained in the Registrar's file

directory hosted by Tormead. Access to these documents will be limited to the Admissions' Team, the Executive Group and, where necessary for support purposes, the IT Team. These documents will be stored in clearly marked directories stored by Intended Year of Entry

Emails are stored in Outlook.

3.5 Do we share admissions personal data with third parties?

We pass details about each girl joining Tormead to Surrey County Council to enable them to maintain their records of children missing from state education. The details shared include the names of girls and their parents, address details, as well as girl's date of birth and previous School.

3.6 Are prospective parents aware of the personal data we process and hold?

Individuals contacting the School regarding Admissions will be made aware of the School's Privacy Policy, which references the data Processing, Storage and Retention Policy, at the point we first capture and retain personal records. Therefore, they will need to acknowledge awareness of this Policy when:

- requesting a prospectus on-line via the School Website;
- booking onto an Open Day via the School Website;mor
- when completing a Registration Form.

Additionally references to the Privacy Policy will be made in the disclaimer text in the School's email footer and will be mentioned during the first phone call with families.

3.7 How do we retain, archive and destroy admissions data?

Tormead needs to retain enquiry and admissions information in RS to support the Admission Process each year and also to facilitate on-going statistical analysis. For example, it is necessary to establish how many enquiries or visits to the School result in registrations, to monitor the ratio of places offered to accepted, and to build relationships with feeder schools etc. Records may need to be held for longer than the seven years recommended for data retention as families enquiring about entry into Reception but who opt to attend other schools, may still potentially be interested in joining Tormead at other entry points all the way up to Sixth Form. Furthermore, as girls only have to register and pay their registration fee once, we may need to keep registration information active for a considerable number of years.

Currently there is no capability with RS to anonymise the historical data that we hold about enquiries and individuals who have been through the admissions process. However, once this functionality becomes available the intended approach to anonymisation will be as follows:

- For general enquiries not resulting in registration, the records will only be anonymised once the prospective pupil has passed the point of entry in to Sixth Form.
- For candidates who register, records will be anonymised three years after the intended year of entry into the School. For example, a record relating to prospective entry in September 2018 which is processed in the 2017-2018 academic year would be deleted at the end of 2019-2020 academic year. The one exception is where parents specifically request that a registration remains active for longer as may be

the case when a candidate who has opted not to join Tormead in Reception would still like to be considered for 11+ entry.

Where candidates accept a place to Tormead, the paper files created to support the Admissions Process are passed to the School Office and are then managed in accordance with the data Processing, Storage and Retention Policy for current pupils. In those instances where places are either not offered or not accepted or the application is withdrawn part-way through the Admissions Process, the paper files are only retained until the end of the academic admissions cycle to which they relate. After this these files are sent for shredding. For example, a file relating to prospective entry in September 2018 would be destroyed at the end of the 2017-2018 Academic Year.

All electronic documents generated by the Admissions Team as part of the Admissions will be deleted three years after the year to which they relate. For example, the documents generated in the 2017-2018 academic year in relation to prospective entry in September 2018 will be deleted at the end of the 2019-2020 academic year.

Any printed documents used to support the Admissions Process which contain personal information will be deleted as soon as they are no longer needed. For example, print-outs displaying prospective parent information that are used during preparation for Open Mornings will be placed in the secure shredding bins as soon as the event has taken place. Likewise any copies of application forms and reference reply forms collated to support the scholarship application process that are shared with teaching staff will be securely shredded once the application process has concluded.

All email correspondence relating to the admissions process will be automatically deleted after three years in accordance with the Tormead email retention policy.

4. CONTRACTORS

4.1 Purpose of this Policy

The General Data Protection Regulation ('GDPR') (effective across the UK from 25 May 2018) impose stricter rules regarding the storage and use of personal data, with the practical effect of requiring more dynamic, efficient and secure storage systems such that:

- All information held by School needs to be justifiable, by reference to its purpose;
- The School must be transparent and accountable as to what it holds, and understand why it holds it;
- Schools must be prepared to respond quickly to subject access requests;
- Contractor data collected should be auditable as far as possible; and
- Contractor data must be held securely and accessed only by those with reason to view it.

The School processes contractor data in accordance with the school's Privacy Notice and the purpose of this section of this Policy is to document how we process, store, retain, archive and destroy contractor data. The School has completed a data audit which has, inter alia, identified the legal bases on which the School processes contractor data, to include:

- compliance with legal / statutory obligations;
- for performance of the contractor contract; and
- for legitimate business interests.

4.2 Which contractor data does this Policy apply to?

Contractors used by the School fall into a number of different categories, and the personal data processed by the School varies by category:

- Outsourced services. Catering, cleaning and the coach service are all outsourced by the School. In order to comply with our statutory obligations, we require the employing company to provide us with written confirmation that all required vetting checks, to include Enhanced DBS, have been completed; we also check identity ourselves, as required by law, and retain copies of the identity documents
- Regular contractors: for a limited number of contractors who are required on site regularly (for example, the electrician) we undertake vetting checks as if they were an employee to enable them to work unsupervised on site. In such cases, we therefore process and hold much of the same personal data as we would for an employee
- Less regular contractors: the vast majority of contractors are not vetted by the School and, should they be required on site while the School is in session, are supervised at all times. Personal data is therefore limited to name, contact details and information required to pay invoices

4.3 What type or records and documents does this Policy apply to?

Records means any document or item of data that includes the personal data of a contractor, and includes both digital and paper records.

As described in section 4.2, the scope of personal data held and processed by the School depends upon the category of contractor.

4.4 How do we store contractor data?

<u>Outsourced services</u>
The contractors provide the HR & Payroll Officer with written confirmation of vetting checks that have been completed, and the contractor's employees provide the HR & Payroll Officer with copies of their identity documents. These are stored in paper form in a secure cabinet accessible only by the Bursar & the HR & Payroll Officer. If information is provided by email, the information is printed off, placed in the file, and the email deleted.

Vetting details for contractors providing outsourced services (currently Holroyd Howe for catering and MAR Services for cleaning) are entered on a separate sheet in the School's Single Central Register. This is filed on the School's secure network in a folder accessible only by the Bursar & the HR & Payroll Officer. When an employee of a contractor leaves, the details are moved to the 'Former Contractors' sheet and are retained indefinitely for safeguarding purposes.

<u>Regular (vetted) contractors</u>
As per employee personal data (see section 1 of this policy).

<u>Non Vetted Contractors</u>
Personal data is limited to name and contact details (and bank details if trading as an individual rather than a company).

The Estates & Facilities Manager has an electronic contact database, and contact details are stored for a maximum of ten years. Contact details and / or payment details on invoices are stored in paper and electronic form for 7 years.

Contractor personal data which may be contained in Health & Safety information and maintenance logs are retained for 10 years. These are held in a secure cabinet accessible only by the Bursar & the Estates & Facilities Manager.

Certain employees of contractors (in particular, employees of contractors providing outsourced services and regular vetted contractors) are required to complete the School's safeguarding training; these training records are stored on the School's secure network.

4.5 Do we share contractor personal data with third parties?

No.

4.6 Are contractors aware of the personal data we process and hold?

Contractors are made aware of the School's Privacy Notice as published on our website.

Contractors providing outsourced services are responsible for advising their employees that, to comply with statutory requirements, they have share personal data of their employees with the School.

4.7 How do we retain, archive and destroy contractor data?

The paper-based and electronic contractor files containing information relating to PPMs and RMs are stored for a period of 10 years, after which they are destroyed using the onsite shredding machine or disposed of in one of four confidential waste bins. We have a 3 year contract with Restore Data Shredding that expires March 2020. Twelve collections are scheduled over twelve months. The confidential waste is then destroyed off site, at one if Restore Data Shred depots.

Any information relating to a Safeguarding matter involving a contractor is stored separately by the Headmistress and is retained indefinitely.

The School's policy is that all emails are deleted after a period of 3 years.

5. GENERAL IT PROCEDURES

All electronic personal data is stored on the School's secure network, save for that personal data which is held on email; the School uses cloud-based Microsoft Office 365 for emails and Microsoft guarantees an EU based server for this. Microsoft's OneDrive / Sharepoint is also used and this data is stored on UK based servers. Google Drive is used only for teaching and other resources which do not include personal data.

The internal network is held behind a powerful firewall, with personal data stored on an internal server and storage in a locked server room. Strict permissions are set for file/folder access. Full backups are performed daily with backups not stored for more than one month.

With one exception, the school's network is accessible only by employees of the School, who must first login to the network with their username and password (network passwords are required to be changed every 90 days and only passwords of sufficient strength are accepted).

Besides School employees, our IT network consultant, Commercial IT, is able to access our network remotely (and thereby access data held on our network). Commerical IT don't have a login for iSAMS, RS, Clarion, LiveRegister, WCBS or WisePay so can't access any information on these secure databases; nor can they access any of our emails, Google Drive or OneDrive content, only the servers themselves. Our relationship with Commercial IT is governed by a Service Level Agreement which has robust confidentiality and data protection provisions.

Electronic files are retained and deleted as set out in previous sections of this policy. Emails are automatically deleted after a period of 3 years running as a nightly process.

Personal data may be held in electronic form in documents created in any of the standard Microsoft Office products (Outlook, Word, Excel and Powerpoint). In addition, the School uses a number of different systems and applications, as follows:

(a) isams

[iSAMS is our MIS system and is used as a database for current and past pupils, attendance registration and reports. Strict permissions are set for different modules.

[iSAMS is contained on two internal servers only accessible by IT for managing updates. The iSAMS database is a secure SQL database store on these servers.

(b) WCBS

PASSFinance, a WCBS product, is the financial software system used by the School. PASS is used to produce and issue all fee statements, and to pay supplier invoices. As such, the system holds personal data of parents, pupils and contractors, with personal data comprising name, parental address, parent email address, contact telephone numbers, date of birth of pupil and, for current parents who pay by Direct Debit, bank account number and sort code.

PASS is only installed on four PCs in the School (that of the Bursar and those of the three members of the Accounts team); login to the system requires a username and password. The PASS database sits on one of the School's secure servers and WCBS can only access remotely by prior arrangement with the School.

Once a pupil leave the School, their data is moved to the 'Past Pupils' section of PASS and the information is retained here for a minimum of 7 years.

(c) Clarion

The School's uses Clarion to communicate with parents via email and text message. There is a nightly secure synchronisation which runs between iSAMS and Clarion synchronising custom groups from Clarion, and pupils/parents information

Any new pupils will have their information synced with Clarion overnight. Old pupil records need to be manually removed when a student leaves the School.

Clarion is a secure web based platform held off site accessible only by the Executive Group and the School Office.

(d) RS Admissions

RS is used for storing personal information of girls and parents before they join the School including names, addresses, phone numbers and previous Schools...

RS is a secure database hosted on an internal server in School. The individual Client folders are located in a server share dedicated to RSAdmissions users with only the user themselves and IT Services having access. Only the registrar, registrar's assistant and Junior Office Secretary can sign in to RS.

Remote access is only available with our express permissions via GoToAssist. We view the screen so there is complete control over what is being done. GoToAssist is blocked by the School firewall unless explicitly allowed for a user.

(e) WisePay

The School uses WisePay to offer parents the option to pay for trips and Sixth Form catering by debit or credit card. Our agreement with WisePay is set out in a Service Agreement. Wisepay's services are hosted and maintained in a UK data centre which is fully compliant and certified to ISO/IEC 27001 and PCI DSS. WisePay is registered as a Data Controller with the ICO, registration number Z1847335.

(f) Live Register

We use the Live Register system to track whether or not Sixth Form pupils are on site at any given time, primarily for Fire Safety purposes. If pupils and their parents have both provided consent, Sixth Formers register at the terminal in the Common Room with their fingerprint; those who have not given consent are issued with a PIN code. Records of consent are maintained and stored by the Head of Sixth Form.

The Live Register system is hosted on the School's secure server and the database is accessible only by the Sixth Form team and IT.

Biometric data is deleted from the system by IT as soon as a pupil leaves - no copies are retained.

Date of Last Review: October 2019