Data Protection Policy

1. Objective

The purpose of this Policy is to ensure compliance with the Data Protection Legislation including GDPR (effective from May 2018) and to ensure that The Harpur Trust discharges all of its legal obligations in this respect.

2. Scope

This policy applies to all activities for which The Harpur Trust is the data controller (see definitions in section 3) and to all Harpur Trust staff (including permanent, temporary and contract staff). The “Harpur Trust” is defined as “all the schools within its legal entity”, therefore requiring only one registration with the ICO. Other activities of the Trust (such as awarding grants and the provision of almshouse accommodation) are also covered in this policy.

3. Definitions

"Data controller" means The Harpur Trust, as an organisation who determine how people's personal data is processed and for what purpose.

"Data subjects" means any living individuals whose data the Data Controller processes.

“Parent or parents” the term ‘parent’ or ‘parents’ should be regarded as including natural parents, step parents, guardians or any other person regarded by the organisation as having a parental role is respect of a future, present or past pupil.

"Processing" means any action in relation to that personal data, including filing and communication.

"Personal Data" includes everything from which a Data Subject can be identified. It ranges from simple contact details via personnel or pupil files to safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's intentions towards that person, and communications (such as emails) with or about them.

"Special category data" are specific categories of Personal Data under the GDPR (broadly equivalent to "sensitive" personal data under the Data Protection Act 1988). These comprise data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health or data concerning a natural person’s sex life or sexual orientation; and biometric data. Extra safeguards are provided by law for processing of such data.

4. Responsibilities

This Data Protection Policy has been approved by, and has the full support of, the Trustees who are ultimately responsible for compliance with data protection legislation.

The Trustees will appoint a Data Protection Officer (DPO) who has direct responsibility for:

- Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws (including maintaining this policy and providing guidance on its implementation).
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, parents etc.).

This role will be performed by the Finance Director based in The Harpur Trust offices.

Each school will appoint a member of their senior leadership team (in most cases, the Bursar/Director of Operations or person in a similar role) who has responsibility for the implementation of this policy within their school and for ensuring that the school's policies and procedures are aligned with this policy. The appointed person will also be the initial contact point for school staff requiring advice and guidance.

All employees will be responsible for implementing the policy within their areas of responsibility. All staff will be provided with education and training appropriate to their roles and will be expected to comply with data protection legislation and adhere to the policies and procedures.

5. Policy statement

It is the policy of The Harpur Trust that:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

There are further detailed policies and procedures which support this Policy, including a Data Breach Policy, a Retention Policy, Information Security Policy and Privacy Notices.

6. Principles

As the data controller, The Harpur Trust is responsible for, and should be able to demonstrate, compliance with the data protection principles under the GDPR.

The following principles shall be complied with throughout The Harpur Trust.

6.1. Lawful basis for processing

6.1.1. The Harpur Trust will determine and document the lawful basis before processing any personal data. The lawful bases will be one of the following:

(a) Consent: the individual has given clear consent for an organisation to process their personal data for a specific purpose. **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

When processing special category data, The Harpur Trust will identify both a lawful basis for general processing and an additional condition for processing this type of data.

6.1.2. The Harpur Trust and Schools privacy notices will include the lawful basis for processing as well as the purposes of the processing.

6.1.3. When asking individuals to provide personal information The Harpur Trust shall be identified as the data controller.

6.1.4. All forms used to collect personal data must clearly state the purpose for which the information is being collected or refer to the appropriate privacy notice where the purpose of the processing is set out.

6.1.5. The Harpur Trust will not use personal data for any purposes other than those advised to individuals directly, those listed in the privacy notices, those detailed in its entries in the Register of Data Controllers published by the Information Commissioner (see Appendix A), or another legal obligation placed on the Trust or the Schools.

6.1.6. The Harpur Trust will obtain the explicit consent of the individual concerned for all processing of sensitive personal data; unless:

- It is information relating to racial/ethnic origin, religion or disability that is being collected purely for monitoring equality of opportunity or treatment
- It relates to the employment of The Harpur Trust staff
- It is necessary for the provision of advice or support and the data subject cannot reasonably be expected to give explicit consent.

6.1.7. The Harpur Trust considers that the consent of students in Year 7 and above (who are deemed mature enough to exercise their own data protection rights) should be sought in addition to parental consent.

6.1.8. The Harpur Trust will require all data processors (outside of the Trust itself) to formally agree that personal data will not be used for any purpose other than the agreed purpose. This will be done by using a Confidentiality Agreement (Appendix B).

6.1.9. The Harpur Trust will not disclose personal data to third parties unless:

- required to by law
- there is an information sharing agreement in place to ensure that any processing by the third party will be within the law (see Appendix C)
- it is necessary in order to fulfil a legitimate purpose that has been advised to the data subject.

6.2. Personal data quality

6.2.1. All forms used to collect personal data shall only ask for information which is relevant to the purpose of the form.

6.2.2. All staff will have the opportunity to view and change the accuracy of personal data held by the HR Department through Employee Self Service.

6.2.3. Changes in personal data relating to pupils, parents and grant recipients must be promptly and accurately updated on the appropriate computer system(s).

6.3. Subject access

6.3.1. The General Data Protection Regulation provides for a right enjoyed by all individuals – including parents, pupils, staff (past, present and prospective) – to know what personal data about them is being held and used by organisations and broadly for what purpose, where it came from, and who else might receive it. This is subject to certain limitations and exemptions.

6.3.2. In order to ensure subject access requests (SARs) are dealt with appropriately, The Harpur Trust Data Protection Officer must be advised of all SARs. Guidance on handling SARS will be issued to each school.

6.3.3. Personal data will only be disclosed to the data subject when:

- The subject access request is made in writing - it does not have to mention GDPR but it should be clear that the requester wishes to access information about themselves, and
- The authenticity of the individual making the request has been confirmed (by requesting any information that is reasonably required to confirm the identity of the requestor).

6.3.4. Requests for access to pupils' files will be co-ordinated with the appropriate Local Data Protection Officer.

6.3.5. A written record of all requests will be created using the subject access response form (Appendix D) and a copy of the form retained in any relevant manual file.

6.3.6. All manual data in relevant filing systems will be reviewed and any personal data relating to 3rd parties either removed, anonymised or consent for its disclosure obtained from the 3rd party.

6.3.7. Responses to subject access requests must include personal data processed by any relevant data processors.

6.3.8. Pupils in Year 7 or above shall be permitted to make subject access requests in their own right, for younger pupils subject access requests must be made by a parent.

6.3.9. All responses to a SAR should be made within a calendar month, starting with the date on which the SAR is received (or the date on which the information referred to in 6.3.3 is received, if later).

6.3.10. The Harpur Trust will exercise the right to exempt information from disclosure if it:

- is legally privileged;
- records the intentions of the Trust or individual school in negotiations with the individual making the SAR;
- consists of a confidential reference given by the Trust or school;
- consists of exam or test answers or exam results before the allotted publication time;
- is held for purposes of management planning (e.g. redundancy planning);
- would prejudice the prevention and detection of crime if disclosed (e.g. in live investigations);
- might cause serious harm or distress (in limited contexts).

6.3.11. Responses to subject access requests will be delivered securely (with effective redactions where necessary). The best way to ensure safe delivery is by agreeing for the requester to collect in person.

6.4. Personal data retention

6.4.1. Personal data shall be retained in accordance with the periods detailed in The Harpur Trust Retention Policy (Appendix E).

6.4.2. Adherence to the Retention Policy, will ensure that personal information is:

- Only held if is justifiable, by reference to its purpose;
- Amended, deleted or transferred promptly upon any justified request, or otherwise the reasons why not are explained;
- Auditable for how the personal data was collected and when; and
- For sensitive data, held securely and accessed only by those with reason to view it.

6.4.3. Staff will review tenancy files whenever accessed and remove and securely destroy any information which is beyond its retention period.

6.4.4. Manual files relating to previous staff, pupils and parents shall have all non-essential information removed and securely destroyed prior to being archived.

6.4.5. The Harpur Trust will require all data processors to formally agree that personal data will not be retained for longer than the purpose for which they are processing it.

6.4.6. In the light of the Independent Inquiry into Child Sexual Abuse (IICSA), The Harpur Trust will not embark on a policy of deleting historic staff and pupil files, or any material potentially relevant for future cases, even if it has been held for long periods already. Data protection should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.

6.5. Staff awareness

6.5.1. All new staff will receive data protection training relevant to their role as soon as possible following the commencement of their employment.

6.5.2. All staff will receive data protection updates and training periodically.

6.5.3. Guidance material will be available to all staff who process personal data. This includes the Harpur Trust's Information Security Policy (Appendix F).

6.5.4. Data protection awareness will be supported by the appointed person within the school/Trust who will receive regular and appropriate training.

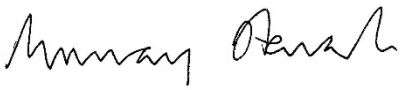
6.6. Data Protection breaches

6.6.1. Any known or suspected data breaches should be reported to the Trust/School if they are 'likely to result in a risk' to the data subject(s) and/or are 'likely to harm individuals'. This will enable the Trust to make the appropriate reports to the Information Commissioners Office (ICO) within 72 hours of becoming aware of a data breach and, where necessary, to inform the affected individuals too. Further guidance on the necessary actions for a data protection breach is set out in the Harpur Trust Data Breach Policy (Appendix G).

7. Governance

The Harpur Trust Data Policy and all supporting policies will be audited periodically as appropriate in order to ensure on-going compliance with data protection legislation.

The policy will be reviewed regularly, at least on an annual basis, by the Data Protection Officer, in conjunction with the Local Data Protection Officers. Any changes will be passed to the Trustees for approval.



Signed …….. (For the Trustees)
Chairman of the Trust

Date ……17 January 2019……..

Appendices

A. Harpur Trust Personal Data Assets register 2018.
B. Confidentiality Agreement
C. Information Sharing Agreement
D. Subject Access Request Form
E. Retention Policy
F. Information Security Policy
G. Data Breach Policy
H.

Personal Data Asset Registers

The Harpur Trust

Staff Admin

Data Subjects	Data Classes	Recipients	Location	Processor
• Staff • Relatives	• Personal details • Education & Training • Employment details • Financial details • Racial or ethnic origin • Trade union membership • Physical or mental health or condition • Offences • Family, lifestyle & social circumstances • Religion • Sexual life • Photographs & images	• Data subjects • Relatives • Current, past, prospective employers • Healthcare, social & welfare advisors • Employees & Agents of the data controller • Financial organisations & advisors • Trade, employer assoc & professional bodies • Central Government • Data processors • Suppliers, providers of goods & services • Local Authorities • Pension Administrators • Criminal Records Bureau • Media	ie • HR Systems • Staff File at School • PASS (fees system) • Intranet (Pupil performance) • ISAMS	ie • BAC • Housing Ass (Alms)

Advertising, Marketing & PR

Data Subjects	Data Classes	Recipients	Location	Processor?
• Staff • Pupils • Complainants, correspondents & enquirers • Suppliers • Advisers, consultants & other professional experts	• Personal details • Family, lifestyle & social circumstances • Goods & services provided • Photographs & images	• Employees & agents of the data controller • Data processors • Media • Persons making an enquiry • Business associates & other professional advisers • Data subjects • Suppliers, providers of goods or services	•	•

Education

Data Subjects	Data Classes	Recipients	Location	Processor?
• Pupils and students • Relatives of the data subject • Staff • Complainants, correspondents & enquirers • Advisors	• Personal details • Family, lifestyle and social circumstances • Performance and behaviour • Education and training details • Goods or services provided • Physical or Mental Health • Racial or ethnic origin • Religious beliefs • Financial details • Employment details • Photographs & images	• Data subjects • Relatives • Employees & agents of the data controller • Healthcare professionals • Examining bodies • Suppliers, providers of goods and services • Debt collection agents	•	•

Educational Support and ancillary services

This purpose relates to provision of boarding services, pastoral care, school trips, etc. Also includes sharing of information with the Foundations and associate organisation related to former pupils.

Data Subjects	Data Classes	Recipients	Location	Processor?
• Pupils • Relatives, guardians and associates of the data subject • Complainants correspondents & enquirers • Advisers, consultants & other professional experts • Suppliers • Staff	• Personal details • Goods or services provided • Racial or ethnic origin • Physical or Mental Health • Education & training details • Family, lifestyle & social circumstances (including behaviour) • Offences • Disciplinary and attendance records • Financial details • Religious belief • Biometric prints/signatures	• Data subjects • Relatives • Employees & agents of the data controller • Suppliers of goods & services • Healthcare practitioners • Organisations linked to the schools	•	•

Schools administration

Data Subjects	Data Classes	Recipients	Location	Processor?
• Pupils • Relatives, guardians and associates of the data subject • Complainants correspondents & enquirers • Advisers, consultants & other professional experts • Suppliers • Staff • Trustees	• Personal details • Goods or services provided • Financial details	• Data subjects • Relatives • Employees & agents of the data controller • Suppliers of goods & services	•	•

Childcare

Data Subjects	Data Classes	Recipients	Location	Processor?
• Pre-school children • Relatives, guardians and associates of the data subject • Complainants correspondents & enquirers • Advisers, consultants & other professional experts • Suppliers • Staff	• Personal details • Goods or services provided • Racial or ethnic origin • Physical or Mental Health • Family, lifestyle & social circumstances (including behaviour) • Financial details • Education and training details • Religious belief	• Data subjects • Relatives • Employees & agents of the data controller • Suppliers of goods & services • Healthcare practitioners • Debt collection agents	• "	•

Accounts & Records

Data Subjects	Data Classes	Recipients	Location	Processor?
• Suppliers • Complainants, correspondents & enquirers • Staff • Trustees • Board Membership • Customers	• Personal details • Financial details • Goods & services provided	• Data Subjects • Employees & agents of the data controller • Business associates & other professional advisers • Suppliers, providers of goods & services • Financial organisation & advisers	•	•

Crime prevention & prosecution of offenders

Data Subjects	Data Classes	Recipients	Location	Processor?
• Staff • Pupils • Relatives • Complainants, correspondents & enquirers • Offenders & suspected offenders • Members of the public • Those inside, entering or in the vicinity of the area under surveillance	• Personal details • Offences (including alleged offences) • Criminal proceedings • Personal appearance and behaviour • Sound and/or visual images	• Data subjects • Employees & agents of the data controller • Police forces	•	

Information & databank administration

This purpose relates to the lists of

Data Subjects	Data Classes	Recipients	Location	Processor?
• Almshouse residents	• Personal details	• Data subjects • Employees & agents of the data controller		

Grants

Data Subjects	Data Classes	Recipients	Location	Processor?
• Applicants	• Personal details • Educational and training details • Financial details	• Data subjects • Employees & agents of the data controller		

Confidentiality Agreement

This is a Confidentiality Agreement between The Harpur Trust, Princeton Court, Pilgrim Centre, Brickhill Drive, Bedford MK41 7PZ (hereinafter "the Discloser" in this Confidentiality Agreement), and Third Party, with an office at Address of Third Party (hereinafter "the Recipient" in this Confidentiality Agreement) under which the Discloser may disclose and the Recipient may receive certain confidential information described in Appendix A and any Addenda thereto, (hereinafter "INFORMATION").

A. CONFIDENTIALITY AND COMMITMENTS

(1) From the date of disclosure, the Recipient shall maintain the INFORMATION in confidence and limit its use to the purposes specified in Appendix A using at least the same degree of care as it employs with respect to the majority of its own confidential information.

(2) The Discloser agrees that the Recipient shall have no obligation with respect to any INFORMATION which:

   a. Is already rightfully known to the Recipient; or
   b. Is or becomes publicly known through no wrongful act of the Recipient; or
   c. Is rightfully obtained by the Recipient from a third party without similar restriction and without breach of this Agreement; or
   d. Is independently developed by the Recipient without breach of this Agreement.

(3) INFORMATION shall not include any third party proprietary or confidential information.

(4) If any INFORMATION is personal data as defined by the Data Protection Legislation including GDPR, then Section B of this Agreement becomes effective.

(5) The Discloser shall retain title to all of the INFORMATION, including INFORMATION provided in the form of computer records, delivered pursuant to this Agreement, and all copies thereof. The Recipient shall not copy or reproduce, in whole or in part, any INFORMATION without written authorisation of the Discloser, except as the Recipient reasonably requires to accomplish the purposes stated in Appendix A. The Recipient shall make reasonable efforts to promptly return or destroy, on written request of the Discloser, all INFORMATION and copies thereof.

(6) The Recipient shall not remove any proprietary, copyright, trade secret, or other legend from any form of the INFORMATION. The Recipient, when reasonably possible and at the Discloser's expense, will add to the INFORMATION any proprietary, copyright, trade secret or other legend or modify same, which the Discloser deems necessary to protect its intellectual property rights and requests in writing to be so added or modified.

B. PERSONAL DATA

(1) All terms underlined in this Section of this agreement will be interpreted using the relevant definitions in the Data Protection Legislation including GDPR

(2) Processing by the Recipient of personal data for which the Discloser is the Data Controller will result in the Recipient being a Data Processor.

(3) Except as expressly provided herein, the Discloser grants no other licence or authority under data protection legislation for the further processing or disclosure of INFORMATION.

(4) Notwithstanding any other provisions of this Agreement, the Recipient agrees not to export, directly or indirectly, any personal data acquired from Discloser to any countries outside the European Economic Area which export may be in violation of the Data Protection Legislation including GDPR. Nothing in this section releases the Recipient from any obligation stated elsewhere in this Agreement not to disclose such data.

(5) The Recipient agrees that appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

(6) The Recipient agrees to grant the Discloser (or its agents) reasonable access to its premises, records and procedures in order that the Discloser may satisfy itself of the adequacy of the security controls implemented by the Recipient in respect of INFORMATION. Such access is subject to the Discloser providing notice in writing at least 20 working days prior to access being required.

C. TERMINATION

(1) The Discloser may terminate this agreement by notifying the Recipient in writing giving 28 days notice.

(2) Upon termination of this agreement the Recipient will return to the Discloser all copies of the INFORMATION in its possession, or provide the Discloser with confirmation in writing that all copies of the INFORMATION have been destroyed securely.

D. GENERAL

(1) This Agreement shall be governed by the laws of England.

(2) This Agreement expresses the entire agreement and understanding of the parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments and understandings pertaining to the subject matter hereof. This Agreement shall not be modified or changed in any manner except in writing and signed by both parties.

(3) If a court of competent jurisdiction finds the provision hereof so broad with respect to time limit as to be unenforceable, such provision may be reduced in scope by the court to the extent it deems necessary to render the provision reasonable and enforceable.

Signed for and on behalf of the Discloser:		Signed for and on behalf of the Recipient:	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Position:	_____	Position:	_____
The Harpur Trust:	_____		_____
Date:	_____	Date:	_____

APPENDIX A

1. The Discloser identifies the following as the INFORMATION:

Description	Format	Classification	Personal Data? (Y/N)
e.g. Tenant contact details	*Excel*	*Confidential*	*Yes*

2. INFORMATION will be used for the sole purpose(s) of:

   Details of purposes for which the data/information may be used

3. The INFORMATION may be used for the defined purpose(s):
   - As a single exercise/operation
   - Until *dd/mm/yyyy*
   - Until further notice

   Amend and/or delete as appropriate

HARPUR TRUST

DATA PROTECTION ACT 2018/GDPR

Subject Access Request Form

This form should be use to make a Subject Access Request under Section 45 of the Data Protection Bill 2018, whereby an individual has the right of access to any personal data held by a Data Controller.

1. Details of Person Requesting the Information

Title (Mr, Mrs, Miss, Dr etc) ..... Date of Birth .....

Surname/Family Name ..... Gender (Male/Female) .....

First Names .....

Maiden/Former Surnames .....

Address .....

..... Postcode .....

Telephone Number (Day) ..... Telephone Number (Evening) .....

Email Address .....

2. Are you the Data Subject:

Yes ☐ If you are the Data Subject, we may ask you to provide one of the following documents: Passport or Driving Licence (go to Section 5)

No ☐ Are you acting on behalf of the Data Subject with their express permission, or with the appropriate legal authority? If so, this must be evidenced in writing and enclosed with this form. We may also ask you to provide one of the documents listed above. Please also enclose proof of the Data Subject's identity described above. Please complete Sections 3 and 4.

3. Details of the Data Subject: (If different to those provided in Section 1)

Title (Mr, Mrs, Miss, Dr etc) ..... Date of Birth .....

Surname/Family Name ..... Gender (Male/Female) .....

First Names .....

Maiden/Former Surnames .....

Address .....

..... Postcode .....

Telephone Number (Day) ..... Telephone Number (Evening) .....

Email Address .....

4. Relationship with the Data Subject (Please briefly describe your relationship with the Data Subject (e.g. Legal Advisor, Spouse) and the reason for you making this information access request on their behalf)

5. Information Required (Please describe as precisely as possible the nature of the information you are requesting, together with any additional information which will help us to locate it, for example: the departments or locations in which it may be held; the nature of your current/past relationship with The Harpur Trust (i.e. pupil/employee); the dates on which correspondence, reports, images or other material may have been created; etc. If you are requesting information within a specific date range then please also indicate this. Please continue on a separate sheet if necessary)

6. Declaration

I certify that the information given on this application form is true and accurate. I acknowledge that it will be used solely for the purpose of processing my request and providing me with my response. I understand that it is necessary for The Harpur Trust to confirm my/the Data Subject's identity and it may be necessary to obtain more detailed information from me in order to locate the correct personal data. I understand that the response period of 1 month, as specified in the Data Protection Act 2018 (section 54).

Signature: ..... Date: .....

Print Name: .....

.....

For official use only

Application signed	Yes ☐ No ☐	Date application received	.....
Application complete	Yes ☐ No ☐	Date further information requested	.....
Identification information provided	Yes ☐ No ☐	Date identification provided	.....
Fee in relation to an excessive request (per s53)	Yes ☐ No ☐	Date information sent	.....
Approved	Yes ☐ No ☐	Number of days to process	.....

Information Sharing Agreement

1. Introduction

The Harpur Trust operates a number of independent sector schools in the Bedford area, provides grants for educational purposes and owns a number of Almshouses, which are managed on its behalf by a local housing association. Each of the schools within the Trust has close links with organisations that maintain links with ex pupils and support the Trust through fund raising activities.

2. Objective

The objective of this Information Sharing Agreement is to establish the circumstances under which information relating to pupils and ex-pupils can be shared with and between these organisations and to define the organisations' responsibilities in complying with the Data Protection Legislation including GDPR.

3. Scope

The Trust operates the following schools within the Bedford area:

- Bedford School (BS)
- Bedford Modern School (BMS)
- Pilgrims Pre-Preparatory School (PPPS)
- Bedford Girls' School

The following table outlines the external organisations that each school maintains a relationship and with which they may share pupil information.

School	External organisation	Activities
BS	Bedford School Foundation	Supports the capital development of the School, funds Scholarships and a variety of other purposes relating to the School.
	Old Bedfordians Club	Networking club for former students of Bedford School. The Club provides the invaluable link between generations of Old Bedfordians and with the School, through an annual programme of social, sporting and networking events and reunions.
	Bedford School Trust	Manages funds which have been bequeathed and donated to the Trust for specific purposes or for the benefit of the School at the discretion of the Trustees. Bedford School Trust also manages a number of funds which are run to support activities within the School.
BMS	Old Bedford Modernians	Enables members to maintain and enjoy the friendships made in their schooldays and promotes the welfare of the School.
BGS	BGS Alumnae	All pupils and staff of Bedford High School and the Dame Alice Harpur School are automatically members of Bedford Girls'

School	External organisation	Activities
		School Alumnae unless they choose not to be. All new pupils to Bedford Girls' School gain membership on joining the school on a lifetime subscription basis. The Alumnae offers a wider range of activities to benefit members of different ages in diverse communities.
	Bedford High School for Girls Foundation	Generates support for bursaries and the capital development of the school by promoting Bedford High School for Girls' achievements and aspirations as a centre of education excellence.
	The Guild	Promotes a feeling of fellowship among past members of the school and aims to maintain and strengthen the friendship between them and the present school.
	Dame Alice Harpur School Association	The Association welcomes into membership all those who wish to remain connected with the school and its community, and offers: • a continued belonging to the Dame Alice community; • the opportunity to share memories at reunions and other social events and through the Association's Newsletter; • news of former pupils and staff information about school life; and • a network link between Association members

This Information Sharing Agreement relates to the sharing of information between the Trust and the external organisations listed above and any subsequent sharing between the external organisations.

4. Personal Information

The personal information relating to pupils and ex-pupils that may be shared under this Agreement is limited to:

- Their name
- Contact details (i.e. address, telephone number(s) and email address)
- The academic years during which they attended the relevant school

It is the responsibility of each organisation to ensure that this information is processed in accordance with this Agreement and any additional personal data is processed in compliance with the DPA.

5. Fair Processing

In its fair processing statement to pupils the Trust makes the following statement:

> *When a pupil joins the school we may pass their contact information to organisations that exist to maintain ongoing contact with ex-pupils. In each pupil's case their contact details will only be provided to organisations linked to the school(s) that they attended.*

External organisations that are party to this Agreement may use the information provided by the Trust for the purpose described above. Should an organisation want to use the information shared under this Agreement for any other purpose(s), it is responsible for ensuring that the fair processing requirements of the First Principle of the Data Protection Legislation including GDPR.are met.

The Trust provides pupils with the right to request that their information is not shared with external organisations and is committed to ensuring that it complies with any such request.

6. Notification

The Trust is a single legal entity and is registered with the Information Commissioner as a data controller. This registration covers the processing of personal data by the Trust, including all of the schools.

Unless exempt from Notification (i.e. use personal data for staff administration, accounts and records or marketing and PR), all external organisations (i.e. parent associations, clubs or foundation) that are party to this agreement must notify the ICO of their processing of personal data as required by Data Protection Legislation including GDPR..

Information and Records Retention Policy: For use by the Schools of The Harpur Trust

The Harpur Trust

November 2018

Introduction

1 This policy sets out a structured approach to reviewing and destroying records in relation to The Harpur Trust (the **Trust**).

2 The retention period for each type of record is shown in the table below. In addition, the Data Protection Legislation (including GDPR) makes it unlawful to keep the information when it is no longer needed for the purpose for which it is held. This requirement is uncertain and allows discretion and may vary according to the circumstances, but in practice it means that the Trust should promptly destroy the record once the retention period in the table below has been reached. Occasionally there may be special circumstances which mean that a record should be kept for longer (for example where there is a risk of a pupil bringing a claim against the Trust). The Trust should refer to its insurance policies and further legal advice should be sought in these circumstances.

3 Information must be securely deleted. This applies to paper records, electronic information and biometric information.

4 This policy does not apply to records connected with commercial activities.

5 The Trust should discuss document retention with its insurers (who may specify longer retention periods). If there is any conflict then any longer retention periods specified by the insurers should prevail.

Emails

6 If an email falls into one of the categories set out in the table then it should be filed centrally as soon as is reasonable.

7 "Routine" emails which do not fall into any of the categories in the table may be kept in inboxes for up to a year and should then be deleted. Examples of routine emails:

7.1 an internal email advising staff that the weekly meeting is cancelled; and

7.2 an internal email attaching a staff rota for an open day.

Independent Inquiry into Child Sexual Abuse (**IICSA**)

8 Specific guidance on retention is also provided from the Independent Inquiry into Child Sexual Abuse (**IICSA**):

8.1 The IICSA (formerly the Goddard Inquiry) has issued retention instructions to a range of institutions regarding records relating to the care of children. In light of this, we are advising schools to temporarily cease the routine destruction of those records which might be relevant to the Inquiry in case they are requested by the Inquiry or made subject to a disclosure order. This means that before destroying any document the Trust should consider if it contains information that may fall within the Inquiry's remit.

8.2 The range of documentation which might need to be kept is wide. It will include any information linked to alleged or established historic child sexual abuse, whether by staff, volunteers or pupils with no limitation date. For example, a list of pupils who attended an overnight school trip or admission registers which show which pupils were at one of the Trust's schools at a given time. As such, documents should be kept for longer than the retention periods listed in the policy if they concern information which might be relevant to the Inquiry.

8.3 Please note that the Trust should keep this under review so that it recommences document destruction at the appropriate time.

Reviewing retention periods

9 At the end of the retention period for each type of record, a review should be undertaken before the records are disposed of. The most appropriate person to conduct this review will depend on the records involved. It should be a person who has the overall responsibility for the records, for example, if the records related to finance, this should be the financial lead (either the Bursar/Director of Operations in the School or the Finance Director for the Trust). The review should take into consideration the following factors:

a) If any record contains a contentious item (e.g. dispute or complaint), the record may be required for longer than the standard retention period;

b) Any record which is still needed for a specific purpose (which would meet the criteria within the data protection regulations) can be retained

10 A record of the rationale for why any document has been retained beyond the standard retention period should be held along with the record itself.

Information and records retention policy

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes (see below for retention period). All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1 In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder. STANDARD DISPOSAL means disposal using waste bins.

2 These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school/trust whilst the school/trust is open.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review as these could be of permanent historical value.	SECURE DISPOSAL
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by Head Teachers, Deputy Head Teachers, Heads of Year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	Admission and parent contract documents including registration form, letter of offer and acceptance form	Yes		Six years from date of leaving the School	Review for further retention in the case of contentious disputes SECURE DISPOSAL
1.3.2	Admissions documents relating to applicants who did not join the Trust	Yes		Minimum one year held at the Trust's discretion. If there is a risk that parents or a pupil might bring a claim against the Trust then the documents should be retained. The documents can be kept for as long as the Trust considers that they are required, subject to the Trust's obligation not to keep the documents for longer than is necessary	SECURE DISPOSAL
1.3.3	Financial information in respect of fees	Yes		Six years from date of leaving the School	Review for further retention in the case of contentious disputes SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.

3. School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 p6

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.5	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General correspondence.	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets/digital records	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide: Keeping children safe in education Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	SECURE DISPOSAL
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	SECURE DISPOSAL
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	SECURE DISPOSAL

2.2 Operational Staff Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File (including references received, annual leave records, contracts and performance reviews etc)	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	If no recent contact from the relevant individual and no apparent breach of contract claim, dispose securely of documentation unless any child protection concerns.
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Single central register	Yes		Current year +6 years. Leavers should be moved on to an archive register (whilst there is no legal requirement to keep details of those staff who have left on the single central register as it is not relevant for inspection purposes, the entry on to an archive register is recommended. This allows us to demonstrate that all checks were carried out prior to work starting).	Review whether further retention is necessary. If so, these reasons must be documented SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children.	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1			Date of warning[6] + 6 months	
	written warning – level 2			Date of warning[6] + 12 months	
	final warning			Date of warning[6] + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

5 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

6 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

2.4 Health and Safety					
Health and Safety – PUPILS					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Accident Reporting / Medical Records	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults (+18 years)			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.4	Reportable injuries, diseases and dangerous occurrences (RIDDOR) reports or own record	Yes		DOB of the pupil involved in the incident + 21 years; or Three years from the date of an incident which may become contentious if the pupil was 18 years old at the date of the incident	Review for further retention in the case of enforcement action or civil claims for personal injury SECURE DISPOSAL
2.4.5	Incident investigations and reports, risk assessments and other relevant documents where there has been an accident or incident			DOB of the pupil involved in the incident + 21 years; or Three years from the date of an incident which may become contentious if the pupil was 18 years old at the date of the incident	Review for further retention in the case of enforcement action or civil claims for personal injury SECURE DISPOSAL
2.4.6	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

Health and Safety – EMPLOYEES					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.7	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.8	Reportable injuries, diseases and dangerous occurrences (RIDDOR) reports or own record			Three years from the date of record If disease - indefinitely	Review for further retention in the case of enforcement action or civil claims for disease or personal injury SECURE DISPOSAL
2.4.9	First aid / accident book entry			Three years from the date of injury or last record in the book If disease - indefinitely	Review for further retention in the case of enforcement action or civil claims for disease or personal injury SECURE DISPOSAL
2.4.10	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year + 40 years	SECURE DISPOSAL
2.4.11	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.12	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL

Health and Safety – employees					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.13	Records of water testing	No		Five years from the date of the last entry	Review for further retention in the case of enforcement action or civil claims for disease or personal injury SECURE DISPOSAL

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Payroll and wage records	Yes		During employment and for a period of six years after employment has ended	SECURE DISPOSAL
2.5.2	PAYE Records	Yes		During employment and for a period of six years after employment has ended	SECURE DISPOSAL
2.5.3	Sickness records required for the purposes of Statutory Sick Pay (SSP)	Yes		During employment and for a period of six years after employment has ended	SECURE DISPOSAL
2.5.4	Records in relation to hours worked and payments made to workers	Yes		During employment and for a period of six years after employment has ended	
2.5.5	An Employee's bank details	Yes		During employment and for a period of six years after employment has ended	SECURE DISPOSAL
2.5.6	Records of advances for season tickets and loans to employees	Yes		Whilst employment continues and up to six years after repayment	SECURE DISPOSAL

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.7	Expression of Wish form	Yes		Whilst employment continues and up to six years after payment of benefit	SECURE DISPOSAL
2.5.8	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.9	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.10	Records and documents relating to membership of and contributions to the Teachers' Pension Scheme	Yes		Indefinitely	N/A

3. Financial Management of the School

This section deals with all aspects of the financial management of the school.

3.1 Risk Management and Insurance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
3.1.2	Other Insurance certificates and schedules of cover			Indefinitely	N/A
3.1.3	Correspondence with insurers related to specific accidents or incidents			Three years generally If the incident involved a pupil - DOB of the pupil involved in the incident + 21 years; or Three years from the date of an incident which may become contentious if the pupil was 18 years old at the date of the incident Disease claims or where there have been allegations of abuse - indefinitely	Review for further retention in the case of civil claims for disease or personal injury SECURE DISPOSAL

3.2 Asset Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Finances					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Finances - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Finances - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Finances – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Finances – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Finances – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Finances - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Meal Records	No		Current year + 3 years	SECURE DISPOSAL

3.6 Bursary applications					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.6.1	Bursary applications	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005 and pupil file	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Pre-Prep and Junior			Retain whilst the child remains at the Pre-Prep and Junior school	The file should follow the pupil when he/she leaves the Pre-Prep and Junior school. This will include: • to another Pre-Prep and Junior school • to a senior or secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be retained for the statutory retention period. If the pupil transfers to a state school, the file should be provided to the Local Authority to be retained for the statutory retention period.
	Senior		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	Review for further retention in the case of contentious disputes, for example, parental complaints, disciplinary matters, pupil exclusions, bullying incidents and Data Protection Act requests SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file and kept for year of exam +7 years	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file and kept for current year +5 years	SECURE DISPOSAL

This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

5.2 Child Protection					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.1	Safeguarding Policies and procedures.	No		Permanent	Transfer to archive for retention when new policy implemented.
5.2.2	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded

5.2 Child Protection					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.3	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	DOB of the child + 50 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	Review for further retention in the case of contentious dispute SECURE DISPOSAL Notes 1 Child protection information must be copied and sent under separate cover to the new school whilst the child is still under 18. Schools should ensure secure transit and confirmation of receipt should be obtained 2 Where a child is removed from roll to be educated at home, the file should be copied to the Local Authority (LA) 3 In accordance with the terms of reference of the Independent Inquiry into Child Sexual Abuse all schools are required to retain information which relates to allegations (substantiated or not) of organisations and individuals who may have been involved in, or have knowledge of child sexual abuse or child sexual exploitation; allegations (substantiated or not) of individuals having engaged in sexual activity with, or having a sexual interest in, children; institutional failures to protect children from sexual abuse or other exploitation. 50 years from the date of birth of the pupil involved should be a sufficient period of retention but this should be kept under review

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Child Protection					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.4	Counselling records held by the School	Yes		DOB of the pupil + 25 years; or Six years from the date of an incident which may become contentious if the pupil was 18 years old at the date of the incident	Review for further retention in the case of contentious disputes SECURE DISPOSAL

5.3 Attendance & Other Records					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	Review for further retention in the case of contentious dispute SECURE DISPOSAL or delete including back-ups and copies
5.3.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL
5.3.3	Biometric information (e.g. fingerprints to be used as part of an automated biometric recognition system)	Yes		For as long as the Trust requires the information for the automated biometric recognition system. This information must not be kept for longer than it is needed. The information must be destroyed if the pupil no longer uses the system including when they leave the School, where a parent withdraws consent or the pupil objects to its use	SECURE DISPOSAL

5.3 Attendance & Other Records					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.4	Documents that are required to be retained for each migrant enrolled under Tier 4 (General) Student or Tier 4 (Child) Student visas			Through the period of sponsorship and for whichever is the shorter period of either: · one year from the date that the Trust ends sponsorship of the Tier 4 student, or · if the Tier 4 student is no longer sponsored, the point at which a Home Office compliance officer has examined and approved the documents	SECURE DISPOSAL

5.4 Special Educational Needs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.4.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.4.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

5.4 Special Educational Needs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.4.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.4.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

5.5 Alumni records					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.5.1	General alumni correspondence, membership forms etc	Yes		Six years after the last time the individual contacted the Trust This is subject to any longer retention period set out above. For example, records relating to a reportable disease which an alumnus has caught should be kept indefinitely in accordance with 2.4.4 above.	SECURE DISPOSAL

5.6 Archive materials					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.6.1	Records which do not contain personal data, for example, old photographs of Trust buildings, title deeds etc			Can be kept indefinitely	N/A
5.6.2	Records relating to a number of pupils, or the Trust generally, such as old class photographs, lists of pupils attending the schools in any given year, School prospectuses, newspaper cuttings etc			Can be kept indefinitely	N/A

5.6 Archive materials					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.6.3	Records concerning specific pupils. For example, a poem written by an exceptionally gifted pupil Routine work produced by pupils should not be kept for longer than the retention periods set out in above unless the Trust has specifically decided to keep it, e.g. for historical purposes and that decision can be justified.			Can be kept indefinitely subject to our comments to the left	N/A

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	

6.2 Implementation of Curriculum					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

8. Work Experience

8.1 Work Experience					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1	Work experience agreements and risk assessments	Yes		DOB of child + 18 years	Retain if a claim arises relating to work experience.

Information Security Policy

Introduction

1. The Harpur Trust operates a number of independent schools in the Bedford area, provides grants for educational purposes and owns a number of Almshouses, which are managed on its behalf by a local housing association. Pupils, their parents, staff and partner organisations look to it to maintain the confidentiality, integrity and availability of their information, some of which may be very sensitive. Information security therefore is extremely important to The Harpur Trust in order to preserve its reputation and to comply with legal and regulatory requirements.

Objective

2. The objective of this Information Security Policy is to protect The Harpur Trust's information assets from all threats, whether internal or external, deliberate or accidental. In support of this objective, the Trustees accept their role in being fully accountable for information security and are committed to:

- Treating information security as a critical business issue
- Creating a security-positive work environment
- Implementing controls that are proportionate to risk
- Achieving individual accountability for compliance with information security policies and supporting procedures.

3. This policy recognises that a core aim of the Trust's schools is the dissemination of knowledge, and that any policy will fail if it assumes that access to the knowledge must, by default, be denied. The policy therefore reflects that the Trust's main concern is to ensure that the steps taken to ensure the integrity of information and, where necessary and appropriate, its confidentiality, are both proportionate and effective.

Scope and definitions

4. The scope of this Information Security Policy extends to:

- All information processed by The Harpur Trust in pursuit of its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
    - Information relating to pupils and their parents
    - Operational plans, accounting records, and minutes
    - Staff records
- All processing facilities used in support of The Harpur Trust's operational activities to store, process and transmit information
- The management of networks located in the Trust and its schools.

5. Within this policy all references to The Harpur Trust shall be regarded as including all of the schools which are part of the Trust as well as activities of the Trust itself.

6. Within this Policy any reference to staff shall be regarded as relating to permanent, temporary and contract staff.

7. Within this Policy the use of the term ‘parent’ or ‘parents’ should be regarded as including natural parents, step parents, guardians or any other person regarded by the organisation as having a parental role in respect of a future, present or past pupil.

8. Within this Policy, the term ‘user’ relates to any staff, pupil, Trustee or any other person authorized to use Harpur Trust computing facilities. These computing facilities include, but are not limited to, Trust/School computers, Trust/School iPads, Trust software and data and the networking elements which link computing facilities.

9. The term ‘system owner’ used within this Policy, is a person (or persons) with overall responsibility for a system and its data as an asset of the Trust.

10. Heads will be accountable for compliance with this Policy within the schools and for ensuring that cost-effective security and legal controls are implemented that are commensurate with the level of risk.

11. The coordination of the management of information security at an operational level will be the responsibility of the Harpur Trust’s CEO who will also be responsible for maintaining this Information Security Policy and providing advice and guidance on its implementation.

12. It is the responsibility of all members of staff to adhere to this Information Security Policy and Appendices 1 and 2. Failure to adhere to this Information Security Policy may involve The Harpur Trust in serious financial loss, embarrassment, legislative action or loss of reputation. Non-compliance by any member of staff may therefore result in disciplinary action. Appendices 3 and 4 apply only to system owners.

Policy

13. As part of its over-arching business strategy and to meet its operational objectives, it is the policy of The Harpur Trust to ensure that:

- Information and information processing assets will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Business requirements for the availability of information and information systems will be met
- Legislative and contractual obligations will be met
- The Harpur Trust’s intellectual property rights and those of others will be protected and respected
- Business continuity plans will be produced, maintained and tested
- Unauthorised use of The Harpur Trust’s information and systems will be prohibited
- This Information Security Policy will be communicated to all staff for whom information security training appropriate to the role will be available
- All breaches of information security, actual or suspected, will be reported to the School Bursar or Harpur Trust Finance Director and investigated.

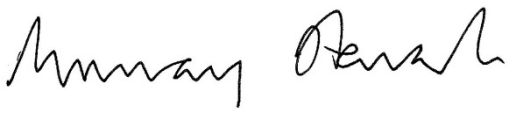
More detailed policy statements and guidance are provided in Appendices 1 to 5 of this Policy.

Risk Strategy

14. The Harpur Trust will follow a balanced information risk strategy aimed at avoiding the unacceptability of high business risks on one side and unnecessarily expensive and bureaucratic controls on the other.

Review

15. This Policy will be approved by the Board and reviewed at least every three years by the Administration and Audit Committee, who will make recommendations on any amendments to the Board.



Murray Stewart
Chairman of the Harpur Trust **September 2017**

Appendices:

1. Detailed policies for all users
2. Password advice and guidance for users
3. Detailed policies and guidance for system owners
4. List of systems and system owners
5. Information Security – ICT Leavers Checklist

Appendix 1 – Detailed policies for all users

The following will be complied with throughout The Harpur Trust.

1. Information Handling

1.1 All users of information systems, including those of servers and personal devices, must manage the creation, storage, amendment, copying, archiving and disposal of information in a manner which safeguards and protects its confidentiality, integrity and availability.

2. Access to information and information systems

2.1 It is the responsibility of system owners to ensure appropriate compliance measures are applied for access to information on their specific system. A list of systems and system owners can be found at Appendix 4. This is current at the time of publishing this policy and is taken to apply to the successive role owner if an employee leaves.

2.2 Access to information must be restricted to authorised users and must be protected by appropriate physical and logical controls.

- Physical controls for information and information processing assets include:
  - Locked storage facilities (supported by effective management of keys)
  - Locks on rooms which contain computer facilities
  - Securing of mobile devices to prevent theft
- Logical controls for information and information processing assets include passwords for systems access and encryption to protect sensitive information either transmitted or taken outside the Trust's properties and/or networks.

2.3 Any username and password or any other access credential issued to a user must be used in accordance with this Policy.

- Passwords should have the following characteristics:
  - A minimum length of 10 characters will be enforced
  - Users must be able to change their passwords at any time
  - Reuse of the 12 previous passwords must be prevented
  - Users should be forced to change their password after a period of 360 days. A minimum password age 0 days will be set.
  - Repeated entry of invalid logon credentials must result in the account being locked. This must be triggered after 500 consecutive invalid attempts.
  - Passwords must be set to include characters from 3 of the following 4 categories:
    - Uppercase letters
    - Lower case letters
    - Base 10 digits (0 through to 9)
    - Non-alphanumeric characters (special characters)

Further guidance on how to set simple but strong passwords is at Appendix 2. It is the responsibility of the user to ensure that passwords meet these characteristics even if it is not possible to configure a system to do this.

2.4 User login information must never be shared with any other person, either directly or indirectly. No user should impersonate another user by using their login information.

2.5 Access to the Trust/Schools' networks shall:

- require staff and pupils (where age appropriate) to authenticate themselves by entering a valid account identifier and password
- be subject to a policy defining the acceptable activities for which the network may be used and defining those things that are specifically forbidden, with all users (where age appropriate) required to formally confirm their understanding and acceptance of the policy

2.6 Access to either Harpur Trust computing facilities or system may be revoked (at the school or Trust's discretion) either temporarily or permanently in the event of non-conformance with the usage policy.

3. Use of Personal Computer Equipment and Removable Storage

3.1 The Harpur Trust recognises that there may be occasions when staff need to use their own computing equipment to process business information (including personal data). To support this, information may need to be stored on removable storage devices (e.g. USB sticks). These practices are permitted provided that the following rules are complied with:

- Users must be aware of the additional risks when using personal computer equipment and/or storage and take appropriate steps to mitigate them. For example, personally owned computers (not including tablets or mobile phones) must have appropriate up-to-date anti-virus software installed and, if connected to the Internet, a firewall.
- Information relating the Trust/school (which includes staff, pupils and parents) must not be saved onto the hard drive of personally owned computers, particularly if it is personal data.
- Removable storage devices must be protected from loss and/or theft using reasonable measures
- Information must not be retained on removable storage devices longer than necessary (i.e. once information that has been updated on a personal computer is uploaded onto the Trust's systems, it must be deleted from the removable storage device).

4. Email and Internet Use

4.1 Detailed policies on staff use of email and the Internet are available to employees via the Trust/school.

4.2 The password that is used to access your school/Trust email account must be unique. Staff should never use a generic password that is used for accessing other accounts or sites. The risk of an attack on the school/Trust is significantly higher if the email system can be accessed via a password which is either used or can be obtained from elsewhere.

4.3 Personal emails must not be accessed on any school/Trust equipment. Any school/Trust equipment should only be used in accordance with the E-Safety Policy. If staff wish to access a personal account during their time at work this must be done via their own device, and not on a school/Trust computer /

tablet e.g. iPad. Doing so significantly increases the risk of infecting the school network with ransomware or other malware.

4.4 The recommended archiving policy for Office 365 packages including e-mail is a period 18 months (or less where appropriate).

5. Mobile Computing

5.1 Use of any mobile computing device owned by the Trust must be in accordance with this Policy.

5.2 Staff with laptop computers and other mobile computing devices must take all reasonable steps to protect these devices from damage, loss or theft. Such steps may include:

- Lock away when not in use
- Never leave laptop computer or mobile devices unguarded in public
- If equipment has to be left in a car, it must be locked in the boot
- Users must take reasonable steps to ensure that confidential information cannot be viewed by unauthorised persons when using computing equipment in public places (e.g. stations, airports, trains, etc.)
- Users must take extra care when using external wireless access points.

5.3 Staff using mobile computing shall be required to ensure that anti-malware products are kept up to date, where possible, automatically.

6. Clear Desk/Clear Screen policy

6.1 Outside normal working hours, all confidential information, whether marked up as such or not, must be secured. No confidential information should be left on desks and unopened mail must be stored away.

6.2 During normal office hours all confidential information, whether marked up as such or not should be secured if desks are to be left unattended for long periods.

6.3 Confidential information must be shredded or placed in an approved confidential waste container.

6.4 Documents which contain confidential or sensitive information should not be left on printers, faxes or photocopiers.

6.5 Outside normal office hours, all desktop computers must be logged off (unless required to remain on for operational purposes).

6.6 Screens should be locked when the user is not at his or her desk.

6.7 Laptop computers other portable assets should be stored securely outside normal office hours.

6.8 Confidential information should not be left unattended in meeting rooms or areas with public access.

7. E-Safety/Safeguarding

7.1 The Harpur Trust reserves the right to access all information (encrypted or unencrypted) where it believes it is reasonable and necessary for safeguarding purposes.

Appendix 2

Password advice and guidance for users

1. Passwords

1.1 Passwords are your protection against your personal, private and business information being compromised and used without your consent. Being hacked can lead to your personal details and those of your friends and colleagues being compromised too. The best defence is herd immunity – everyone keeps everyone else secure.

1.2 A common tactic of hackers is to attack an easy password and use that access to gain access to other passwords and so on. This can lead to you're a serious breach of your security and leaking data relating to confidential work. It is your duty and responsibility to take reasonable precautions to protect yourself, your colleagues and the school.

- Do you find passwords hard to remember?
- Do you have password containing names and numbers? Fred99, Janice68 etc.
- Does your password or PIN number contain your date or year of birth?
- Do you have simple passwords of one word and a number?
- Do you use a variant of your username as your password?
- Do you re-use passwords between different sites?
- Do you keep emails with passwords in your email Inbox?

1.3 These are all common issues that can be addressed using a simple approach. In theory a 4-number PIN has 9999 different combinations. It has been shown that where people use common sequences such as dates, or repeated numbers (2222, 3333, etc.) these combinations can be reduced to 100s or even 10s. This makes them guessable.

1.4 If you use the same PIN number or password for multiple systems then your details can be re-used and access can be gained across different systems. If someone gains access to your email and then resets your password by sending a link to your email then they have access to that system as well. In this way your bank, your social media accounts, your personal and work records can all be accessed.

1.5 Hackers will routinely try a list of passwords containing many lists of commonly used passwords in multiple languages, including variations like P@55W0Rd or similar. They can try hundreds of thousands of these a minute with automated systems designed to crack passwords. A short password (7 characters or less) can be hacked in a matter of hours even if it is completely random.

1.6 Click the link below for a list of the most commonly used passwords.
http://www.passwordrandom.com/most-popular-passwords

1.7 So what can you do?

Making a better password involves:

- It must be hard to deduce or guess
- It must be easy to remember
- It must be easy to enter (on PC, Tablet, Phone)

1.8 What if you could have an easy to remember password that is difficult to guess or predict?

1.8.1 **Better Passwords**

A better password is ten or more characters long and contains numbers, upper and lower case characters and punctuation. You might think this would be difficult to remember but it needn't be:

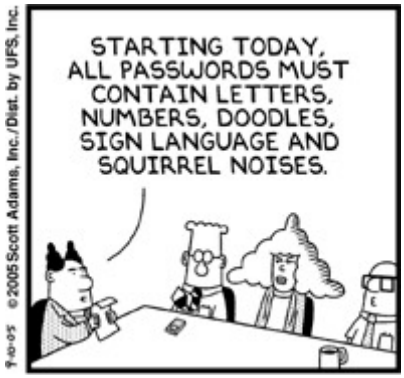
- Purple.Elephant.H2O
- Zero-Emit-Radio
- Turbo-Fruitcake-365
- Animated.bingo.wins

1.9 These are examples of good passwords that are extremely hard to guess but relatively easy to remember and easy to type into a mobile device. With three easy to remember words it is possible to come up with a unique address for every location on the planet, as demonstrated here:

http://what3words.com/
(please do not use your address location for a password as that too would be like using your postcode and is easy to guess for anyone who can look you up).

1.10 So using three simple words and a separating character you can easily generate a memorable, easy to use, secure password. You can then have separate passwords for different services you are using so that you don't, for instance, use the same password for the School MIS as you do for Email.

1.11 If you have any concerns about network security or would like help changing your password, then please feel free to come to IT Support and we will assist. Many thanks for your help in keeping the Trust secure.



Appendix 3 Policy for system owners

The following will be complied with by system owners within The Harpur Trust.

1. Access to information and information systems

1.1 It is the responsibility of system owners to ensure appropriate compliance measures are applied for access to information on their specific system. A list of systems and system owners can be found at Appendix 4. This is current at the time of publishing this policy and is taken to apply to the successive role owner if an employee leaves and before the policy is updated.

1.2 Access privileges will be allocated to staff based on the minimum privileges required to fulfil the users' job function. Access privileges shall be authorised by the appropriate system owner (or to a person/s to who the System owner has delegated approval responsibility to, for example during their absence or for practical reasons).

1.3 Access to school systems provided to parents must employ sufficient controls to ensure the confidentiality, integrity and availability of information which is available on these systems.

1.4 All access permissions should be granted, amended and revoked following an appropriate access authorisation process.

1.5 System owners shall review access permissions on an annual basis.

2. Information Backup

2.1 The requirements for backing-up information should be defined based upon how often the information changes and the ease with which lost data can be recovered and re-entered.

2.2 The IT staff responsible for each location, along with the system owners, are responsible for ensuring that systems and information is backed up in accordance with the defined requirements.

2.3 Accurate and complete records of the back-up copies must be produced and maintained.

2.4 The back-ups must be stored in a remote location which should:

- be a sufficient and reasonable distance to escape any damage from a disaster at the main site
- be accessible within normal working hours
- afford an appropriate level of protection during storage and transportation to and from the remote location

2.5 Back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.

2.6 Restoration procedures (i.e. the retrieval of a previous version of information) should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

3. Leavers

3.1 It is recommended that an ICT Leavers checklist (Appendix 5) is completed to ensure that accesses are removed, information is transferred and IT equipment recovered. The ICT Leavers checklist should be completed and forwarded to the ICT Department.

Appendix 4 List of systems owners and access

Systems	Location	Owner
Payroll **(iTrent)**	HTO/Schools	Clare Lake
Accounts **(eBIS/Open Account)**	HTO/Schools	Clare Lake
Fees **(PASS)**	HTO/Schools	Clare Lake
HR **(iTrent)**	HTO/Schools	Sam Lock
Grants **(Benefactor)**	HTO	Lucy Bardner
Fundraising & Alumni Relations **(Donor Strategy)**	BMS	Julie Ridge (Director of External Relations)
Fundraising & Alumni Relations Raiser's Edge	BGS	Jemma Trobe
Fundraising & Alumni Relations Raiser's Edge & Net Community	BS	Richard Garrett
iSAMs	BMS	Richard Pooley
MIS (iSAMs)	BS	Peter Drage
MIS (Capita SIMS)	BGS	John Gardner
Admissions RS Admissions	BS	Richard Midgley
MIS **RS Admissions**	BGS	Jemma Trobe
Library**(Heritage Cirqa)**	BMS	Angelo Felice

Systems	Location	Owner
Library **(Heritage Cirqa)**	BS	Lesley Harrison
Library **(Autolib – Payne Automation)**	BS	Lesley Harrison
Cashless Catering System **(Impact)**	BMS	Angelo Felice
Pupil and Staff Biometric Database System **(Biostore)**	BMS	Angelo Felice
Pupil Biometric Database System (Biostore)	BS	Lesley Harrison

Appendix 5

The Harpur Trust
Information Security – ICT Leavers Checklist

Leaver's Details	
Name: ..... Department:	
Date leaving: ..... ☐ Teacher ☐ Support Staff	
ICT Checklist	
Action	**Date Completed**
Identify all documents and tasks for which the individual is responsible and ensure transfer to relevant person (if required).	
Ensure all information from personal areas and local drives are transferred or deleted.	
Ensure all emails that required action are transferred to relevant person.	
Unsubscribe from any electronic or manual mailing lists.	
List all systems or services used (overleaf) so that the ICT Department can change/disable or delete logins.	
ICT Department must remove email access.	
Identify and recover all trust ICT equipment (list overleaf) which is in the user's possession.	
Identify and transfer any ICT duties, such as changing backup tapes, checking backup logs or system administration. (ICT staff only)	
Consider changing any system related subscriptions/contract passwords (ICT staff only).	
Consider changing system administrator account passwords (ICT staff only)	
Remove entry from the intranet, internet or any other contact/distribution lists/directories (if necessary).	
Change Voicemail Message (if applicable).	
Recover all security badges, door or filing cabinet keys and activations passes.	
Consider alarm codes for security systems within The Trust (if known by the leaver).	
Notify HTO IT Department staff of the financial applications used.	

Please note this list is not exhaustive and can be added to using a separate sheet and attaching it to this form.

Identified Equipment							
Tick all that have been identified as in the user's possession whilst working for The Trust.							
☐	Laptop/netbook	☐	Smartphone/PDA	☐	Mobile Phone	☐	Printer
☐	Home installed PC	☐	USB key/Flash Drive	☐	Software Media i.e. CDs		
☐	Other (please state):						

Returned Equipment		
Description of Equipment	**Received by**	**Date returned**

Systems or Services Used

Declaration:			
Please ensure that you have completed all the sections			
Manager's Name (Printed):			
Manager's Signature:		Date	.....
Leaver's Name (Printed):			
Leaver's Signature:		Date	.....

Data Breach Policy and Procedure

To be used following an actual or suspected data breach

The Harpur Trust

November 2018

1 Introduction

1.1 The Trust understands the importance of keeping personal data secure and of effectively dealing with data breaches. This is essential for maintaining the trust of staff, pupils and their parents when the Trust uses their information.

1.2 This policy and procedure is to be used by the Trust's Governance Sub-Committee in the event of a data breach at the Trust (or a suspected data breach). The Sub-Committee is comprised of the senior members of staff who will deal with different aspects of a data breach.

1.3 All staff should receive training on how to recognise a data breach and the Trust's Information Security Policy contains guidance for staff on this issue.

1.4 The Trust is required to report certain breaches to the Information Commissioner's Office (ICO) and to data subjects under the General Data Protection Regulation (GDPR). There are strict timescales for reporting breaches which are outlined in section 7.

1.5 The Trust also has responsibilities to report certain incidents to other regulators such as the Charity Commission. Section 7 below covers these reporting obligations.

2 Definitions

2.1 The following terms are used throughout this policy:

Trust – The Harpur Trust

School – Any of the schools which belong to The Harpur Trust, including Bedford School, Bedford Modern School, Bedford Girls' School and Pilgrims Pre-Preparatory School (including Little Pilgrims).

3 Immediate action following a data breach

- Inform all members of the Governance Sub-Committee.
- Identity what personal data is at risk.
- Take measures to prevent the breach from worsening e.g. changing password/access codes, removing an email from pupils' inboxes which was sent by mistake.
- Recover any of the compromised personal data e.g. use back-ups to restore data.
- Consider whether outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm being caused to a pupil.
- Consider whether any affected individuals should be told about the breach straight away. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals covered at 8.6 – 8.10 below which does not need to be an immediate notification.

4 What is a data breach?

4.1 A data breach is a breach of security which leads to any of the following:

4.1.1 the loss of personal data;

4.1.2 the accidental or unlawful destruction of personal data;

4.1.3 the disclosure of personal data to an unauthorised third party;

4.1.4 the unlawful or accidental alteration of personal data; or

4.1.5 unauthorised access to personal data.

4.2 Personal data is information:

4.2.1 from which a person can be identified (either from the information itself or when combined with other information likely to be used to identify the person); and

4.2.2 which relates that person.

4.3 The following are examples of personal data held by the Trust:

4.3.1 names and contact details of pupils, parents and staff;

4.3.2 financial information about parents and staff;

4.3.3 pupil exam results;

4.3.4 safeguarding information about a particular family;

4.3.5 information about pupil behaviour and attainment; and

4.3.6 a pupil or staff member's medical information.

4.4 If staff are in any doubt as to whether an incident constitutes a data breach they must speak to the Operational Lead at the school or the Finance Director immediately.

4.5 Please see Appendix 1 for examples of data breaches.

5 Roles and responsibilities

5.1 The following staff form the Trust's Governance Sub-Committee (the **Committee**) and will have certain responsibilities:

Role	**Responsibility**
The Finance Director	The Finance Director (FD) is responsible for co-ordinating the Trust's response to any breach. In addition, the Finance Director will lead on any physical security measures which are required at the Trust site to contain the breach. The Finance Director is responsible for notifying and liaising with the Trust's insurers as required. If the breach has taken place at one of the Schools, the FD will contact the Operational Lead of the relevant school to manage the breach and ensure any possible technical measures are taken to recover any personal data or to

	contain a data breach. The Finance Director will instruct the relevant IT team to ensure the security of the Trust's ICT infrastructure and to ensure any possible technical measures are taken to recover any personal data or to contain a data breach.
The Operational Leads	The Operational Leads of the affected School will be responsible for any communications with pupils and parents and for liaising with the Head for any pupil welfare or disciplinary considerations.
The HR Director	The HR Director will lead on any employee welfare or disciplinary issues in consultation with the Head and/or Operational Lead. This will only happen if the breach is serious and requires disciplinary action.
The Chief Executive	The Chief Executive will be responsible for liaising with the Trustees or Governors as appropriate. Any decision to report the data breach to the Charity Commission will be taken by the Trustees.

5.2 The Committee will form as soon as possible once a data breach has been identified.

6 Containment and recovery

6.1 As soon as a data breach has been identified or is suspected, steps must be taken to recover any personal data and to contain the breach. For example, the Trust/Schools may need to:

6.1.1 change any passwords and access codes which may have been compromised;

6.1.2 if appropriate in all the circumstances, tell employees to notify their bank if financial information has been lost (or other information which could lead to financial fraud) and offer credit protection;

6.1.3 limit staff and/or pupil access to certain areas of the Trust's/School's IT network(s);

6.1.4 use back-up tapes to restore lost or damaged data;

6.1.5 take any measures to recover physical assets e.g. notifying the police or contacting third parties who may have found the property; and

6.1.6 notify its insurers; and

6.1.7 take action to mitigate any loss.

6.2 The Committee should decide what action is necessary and which member(s) of the Committee will be responsible for the different aspects of the containment and recovery. Where appropriate the Committee will delegate tasks to other members of staff with the relevant expertise.

6.3 The Committee should seek assistance from outside experts if appropriate to effectively contain the breach and recover any personal data. For example, legal advice, reputation management advice or specialist technical advice.

7 Establishing and assessing the risks

7.1 The next stage in the process of dealing with a data breach is to establish and assess the risks presented by the breach. To assist with this process, the Committee should document the answers to the questions contained in Appendix 2 in as much detail as possible.

7.2 The table in Appendix 2 should be copied into a new document in order to retain a record of this process.

8 Notification

Notification to the Information Commissioner's Office

8.1 From 25 May 2018 the Trust will be required to report a data breach to the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. The exercise which was documented under section 6 above should be used to determine if a notification to the ICO is required.

8.2 "Risk to the Rights and freedoms of individuals" should be interpreted broadly. Please see row 5 of Appendix 2.

8.3 Any decision to not notify the ICO should be documented. It is possible that if another data breach occurs in the future that the ICO will ask why any previous breaches were not reported and the ICO is likely to ask to see evidence of any decision to not notify.

8.4 If the Trust decides to notify the ICO then this must be done without undue delay and where feasible within 72 hours of having become aware of the breach.

8.5 Content of the notification

8.5.1 The ICO has set out procedures for notifications on their website (ico.org.uk) which should be followed.

(a) However, the Trust should also prepare a letter to the ICO in addition to following the ICO's procedures on the website in all but the most minor breaches because this provides the opportunity to present what has happened in a way that is advantageous to the Trust.

(b) The Trust may need to send this letter after the initial notification to incorporate any subsequent action taken by the Trust which may act in mitigation against ICO enforcement action.

8.5.2 The notification must contain as a minimum:

(a) a description of the nature of the data breach including where possible:

(i) the categories and approximate number of data subjects concerned; and

(ii) the categories and approximate number of personal data records concerned.

(b) the name and contact details of the Finance Director who can provide more information to the ICO if required;

(c) a description of the likely consequences of the data breach;

(d) a description of the measures taken or proposed to be taken by the Trust to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.5.3 If it has not been possible to submit the notification to the ICO within 72 hours of becoming aware of the breach, the notification must explain the reason for this delay. For example, that the Trust has been instructed by the police to postpone the notification to the ICO.

8.5.4 If it is not possible to provide all of the information at the same time, the Trust should provide the information to the ICO in phases without further undue delay. For example, the Trust could make an initial notification within the 72 hour period with a more detailed response the following week once the Trust has more information on what happened.

8.5.5 The initial notification should include points such as the possible cause of the breach and how the Trust plans to deal with the breach including mitigation actions.

8.5.6 The more detailed response should set out as clearly as possible the steps the Trust has taken to prevent a reoccurrence. The ICO is less likely to take enforcement action if it considers that the Trust has already taken steps to address what went wrong.

Contacting affected individuals

8.6 The Trust is required by the GDPR to report a data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals. It may not always be clear which individuals should be notified, for example, parents may need to be notified rather than their children.

8.7 The Trust should use the exercise at section 6 above to assist with this decision. A notification does not need to be made where:

8.7.1 the Trust had taken measures so that the data compromised was unintelligible to any person not authorised to access it (e.g. it was encrypted); or

8.7.2 the Trust has managed to contain the breach or take mitigating action so that any high risk to individuals is no longer likely to materialise (e.g. an unencrypted memory stick has been recovered before anyone was able to access the data held on it).

8.8 If the Trust decides not notify individuals this decision must be documented.

8.9 If a notification is sent this must be done so without undue delay. The Trust should work with the ICO in determining when is the most appropriate time to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification.

8.10 The ICO may advise or require the Trust to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals. The ICO is given these powers under the GDPR.

8.11 **Content of the notification to individuals**

8.12 The notification to individuals must include the following as a minimum:

8.12.1 the name and contact details of a person at the Trust who can provide more information. The appropriate staff member at the Trust should be chosen by the Committee and is likely to depend upon which individuals are affected;

8.12.2 a description of the likely consequences of the data breach; and

8.12.3 a description of the measures taken or proposed to be taken by the Trust to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.13 In addition, the Trust must consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

8.14 The notification must be drafted in clear language. If directed at pupils the notification should be age appropriate.

8.15 The Committee should decide what is the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

Serious Incident Report to Charity Commission

8.16 The Charity Commission's guidance makes it clear that serious incidents should be reported to it as soon as possible. Where there has been a data breach, the Governors will need to consider whether to make a serious incident report to the Charity Commission.

8.17 In a press release dated 9 December 2016, the Commission set out a specific expectation that where a notification is made to the ICO, a charity will make a serious incident report to the Charity Commission. The Charity Commission has extensive information sharing powers with other regulators, like the ICO, so the Commission may be aware if a serious incident report is not made.

8.18 Because of the breadth of the Charity Commission's criteria for making serious incident reports, Governors should consider whether to make a report in light of the data breach and surrounding circumstances - even where it has not been necessary to notify the ICO.

Notification to the police

8.19 The Trust should consider whether the police need to be notified about the data breach because it is possible that a criminal offence has been committed. However, there is no legal obligation to notify the police. The following are examples of breaches where a criminal offence may have been committed:

8.19.1 theft e.g. if a laptop has been stolen;

8.19.2 burglary;

8.19.3 if a staff member has shared or accessed personal data where this was not required as part of their professional duties e.g. a staff member shares information about a pupil with famous parents with the local press;

8.19.4 the Trust's/School's computer network has been hacked (e.g. by a pupil or a third party).

8.20 Action Fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk

9 Internal Breach Register

9.1 The Trust is required to keep a register of all data breaches including those which do not meet the threshold to be reported. Staff should be trained to report all data breaches to allow the Trust to meet this requirement.

9.2 The Finance Director is responsible for keeping this register up to date.

10 Evaluation

Evaluation of the Trust's security measures

10.1 The Trust is obliged under the GDPR to implement technical and organisational measures to protect personal data. The Trust regularly evaluates of the effectiveness of both its organisational and technical measures.

10.2 Organisational measures include:

10.2.1 policies for staff on their data protection obligations, including when working away from the Trust/School site;

10.2.2 guidance for staff on how to use specific computer applications and software securely; and

10.2.3 data protection training for staff.

10.3 Technical measures include:

10.3.1 the use of encryption;

10.3.2 limiting access to certain areas of the Trust's/School's IT network;

10.3.3 firewalls and virus protection; and

10.3.4 the use of backups.

10.4 The Committee should establish how the existing measures could be strengthened and what additional measures should be put in place to guard against future data breaches. The Committee should consider both breaches of a similar type to that which has occurred and the risk of security breaches more broadly.

10.5 The Committee may delegate this task to one or more appropriate members of staff. The Committee should consider whether legal and/or technical advice is required.

10.6 This exercise should be undertaken promptly because the actions taken by the Trust (including the Schools)to improve its practices will likely be taken into account by the ICO when considering if enforcement action should be taken against the Trust

10.7 Key points to consider include:

10.7.1 Would improvements in the training given to staff have prevented the breach or lessened the severity of the breach?

10.7.2 Can measures be taken to speed up the process of staff reporting breaches?

10.7.3 Does the Trust's Information Security Policy need to be revised?

10.7.4 Are changes required to the Trust's/School's IT system?

10.7.5 Should the Trust's/School's document management system be made more robust? For example, should staff's ability to access certain documents be limited to a greater extent.

10.7.6 Does the physical security of the Trust/School, particularly in areas where personal data is kept, need to be improved?

10.7.7 Do the Trust's/School's remote working practices need to change?

10.7.8 Does the Trust/School need more robust procedures around staff using their own devices for Trust/Schoolwork?

10.7.9 Do the Trust's/School's contracts with processors (e.g. a Cloud storage provider) need to be revised?

10.7.10 Does the Trust/School need to do more robust due diligence on its processors?

10.7.11 If any IT services providers were contracted by the Trust/School to carry out work related to information security was the service provided adequate?

10.8 The Committee should report the outcome of the evaluation to the Administration and Audit Committee before implementing any necessary changes.

Evaluation of the Trust's response to the data breach

10.9 When the immediate action has been taken following the data breach, the Trust should evaluate how its initial response to the breach could have been better.

10.10 Key points to consider:

10.10.1 Was the breach reported to the Finance Director immediately? If not, what action can be taken to speed up the process of contacting a senior member of staff.

10.10.2 Were all possible measures taken to recover the data promptly?

10.10.3 Could more have been done to contain the breach as quickly as possible?

10.10.4 If one of the Trust's/School's processors (e.g. a payroll supplier) was either responsible for the breach, or discovered the breach, was this notified to the Trust/School without undue delay? If not, what measures can be put in place to improve this communication in the future?

10.11 The Committee should report the outcome of the evaluation to the Administration and Audit Committee before implementing any necessary changes.

11 Tactical considerations

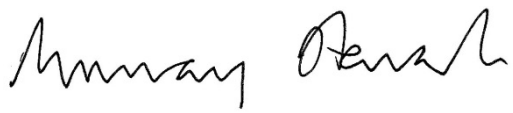
11.1 The Trust should refer to Appendix 4 which outlines tactical and supplemental considerations. For example, is any pupil disciplinary action required?

12 Monitoring and review

12.1 The Finance Director should ensure that this policy is regularly reviewed and updated as required.

12.2 This policy should be reviewed following any data breach at the Trust which meets the threshold to be reported to the ICO.

12.3 This Policy will be approved by the Board and reviewed at least every three years by the Administration and Audit Committee, who will make recommendations on any amendments to the Board



Murray Stewart
Chairman of the Harpur Trust **November 2018**

Appendices:

Appendix 1 Examples of data breaches and the next steps

Appendix 2 Establishing and Assessing the Risks Presented by the Data Breach

Appendix 3 External advice

Appendix 4 Tactical and supplemental considerations

Appendix 1 Examples of data breaches and the next steps

Example of breach	Containment and Recovery	Establishing and Assessing the Risks	Notification	Evaluation of the Trust's response to the data breach
A staff member leaves papers containing information about pupils' academic performance on a train. The papers were not in a locked case.	The Trust should find out if it is possible to retrieve the papers. For example, by calling the train company's lost property department.	The Trust should work through the questions in Appendix 2 below.	If the papers are not retrieved then this breach will need to be notified to the ICO. Whether a notification to the pupils and their parents is required will depend upon the nature of the personal data. The Trust should consult section 7 of this policy.	The Trust should work through sections 9.9 to 9.11 of the policy above.
Ransomware locks electronic files containing personal data.	The Trust should have a back-up of the data and should also ensure that its systems are secured (e.g. that the ransomware has been removed).	Ditto	Depends on factors such as whether the Trust was able to recover the data and whether there is any other risk to the Trust's systems	Ditto
Sending an email containing personal data to the incorrect recipient.	Use the recall email feature if available. Consider calling the unintended recipient and ask them to delete the email	Ditto	Depends on the sensitivity of any personal data contained in the email, whether the unintended recipient has agreed to delete it etc.	Ditto

Appendix 2 Establishing and Assessing the Risks Presented by the Data Breach

	Question	Response
1.	Precisely what data has been (or is thought to have been) lost, damaged or compromised?	
2.	Is any of the data Critical Trust Personal Data as defined in the Trust's Data Protection Policy? This would be: i. information concerning child protection matters; ii. information about serious or confidential medical conditions and information about special educational needs; iii. information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved); iv. financial information (for example about parents and staff); v. information about an individual's racial or ethnic origin; and vi. political opinions;	

	vii. religious beliefs or other beliefs of a similar nature; viii. trade union membership; ix. physical or mental health or condition; x. genetic information; xi. sexual life; xii. information relating to actual or alleged criminal activity; and xiii. biometric information (e.g. a pupil's fingerprints following a criminal investigation). If any of these types of data are involved this makes the breach more serious.	
3.	Who are the affected individuals e.g. staff, parents, pupils, third parties?	
4.	How many individuals have definitely been affected and how many potentially affected in a worst case scenario?	
5.	What harm might be caused to individuals (not to the Trust)? The individuals do not necessarily need to be	

	those whose personal data was involved in the breach. Harm should be interpreted broadly, for example to include: (a) distress; (b) discrimination; (c) loss of confidentiality; (d) financial damage; (e) identity theft; (f) physical harm; and (g) reputational damage.	
6.	What harm might be caused to the Trust? For example, reputational damage and financial loss.	
7.	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point. (a) Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen?	

	(b) Were any technical protections in place e.g. was the data protected by encryption? (c) Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? (d) Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	

Appendix 3 External advice

Legal advice

The Trust should consider taking legal advice in relation to the following. Please note that this is not an exhaustive list but should be used as a guide.

1. Determining whether to notify the ICO and the data subjects.
2. Drafting the notification to the ICO and the data subjects.
3. Drafting a serious incident report to the Charity Commission.
4. Any correspondence with other external agencies such as the Independent Trusts Inspectorate or the Department for Education.
5. Any communications with the police.
6. The decision to notify the Trust's insurers.
7. Any communications with staff members, pupils and parents.
8. Any disciplinary action in relation to pupils or staff.
9. Establishing whether there is a risk that an affected individual might bring a legal claim against the Trust.

Reputation management

The Trust should consider obtaining advice regarding reputation management. This advice may be provided by solicitors or by other specialists. As above, this is not an exhaustive list but should be used as a guide.

The following circumstances in particular may require specialist advice:

1. If the data breach becomes widely known to the parental community.
2. If news of the breach becomes known outside of the Trust community.
3. If the media report on the breach or ask the Trust for a statement.
4. If the ICO take enforcement action which may become public knowledge.

Appendix 4 Tactical and supplemental considerations

This appendix should be completed to assist the Trust in checking that all issues surrounding the data breach have been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the data breach.

Supplemental issue	**Considerations**
Pupil welfare	
Staff welfare	
Parental complaints	
Staff disciplinary action	
Pupil disciplinary action	
Reputation management	
Risks of legal claims	
Possible Charity Commission action	