

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.

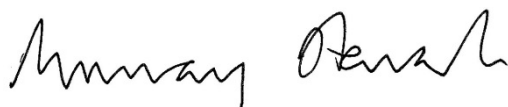
More detailed policy statements and guidance are provided in Appendices 1 to 5 of this Policy.

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
of the Harpur Trust

September 2020

Chair

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 For any shared systems (i.e. used by multiple locations across the Trust), the system owners will agree an appropriate “Code of Conduct” for all users of that system (i.e. password length and frequency, access methods) to ensure there is no potential weak point which would expose the security of another site.
- 2.3 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.
- 2.4 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.

- 2.5 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.
- 2.6 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
- 2.7 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.
- 5.4 All employees who are working from home should be provided with appropriate guidance on how to keep business information confidential, in the same way as it is within the workplace.

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
Payroll (iTrent)	HTO/Schools
Accounts (eBIS/Open Account)	HTO/Schools
Fees (PASS)	HTO/Schools
HR (iTrent)	HTO/Schools
Grants (Benefactor)	HTO
Fundraising & Alumni Relations (Donor Strategy)	BMS
Fundraising & Alumni Relations Raiser's Edge	BGS
Fundraising & Alumni Relations Raiser's Edge & Net Community	BS
iSAMs	BMS
MIS (iSAMs)	BS/PPPS
MIS (iSAMS)	BGS
Library(Heritage Cirqa)	BMS

Systems	Location
Library (Heritage Cirqa)	BS
Library (Autolib – Payne Automation)	BS
Cashless Catering System (Impact)	BMS
Pupil and Staff Biometric Database System (Biostore)	BMS
Pupil Biometric Database System (Biostore)	BS



The Harpur Trust Information Security – ICT Leavers Checklist

Leaver's Details	
Name: Department:	
Date leaving:	<input type="checkbox"/> Teacher <input type="checkbox"/> 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.

<input type="checkbox"/>	Laptop/netbook	<input type="checkbox"/>	Smartphone/PDA	<input type="checkbox"/>	Mobile Phone	<input type="checkbox"/>	Printer
<input type="checkbox"/>	Home installed PC	<input type="checkbox"/>	USB key/Flash Drive	<input type="checkbox"/>	Software Media i.e. CDs		
<input type="checkbox"/>	Other (please state):						

Returned Equipment	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

Description of Equipment	Received by	Date returned

Systems or Services Used	
1	1.1
2	2.1
3	3.1
4	4.1
5	5.1
6	6.1
7	7.1
8	8.1
9	9.1
10	10.1
11	11.1
12	12.1
13	13.1
14	14.1
15	15.1
16	16.1
17	17.1
18	18.1
19	19.1
20	20.1
21	21.1
22	22.1
23	23.1
24	24.1
25	25.1
26	26.1
27	27.1
28	28.1
29	29.1
30	30.1
31	31.1
32	32.1
33	33.1
34	34.1
35	35.1
36	36.1
37	37.1
38	38.1
39	39.1
40	40.1
41	41.1
42	42.1
43	43.1
44	44.1
45	45.1
46	46.1
47	47.1
48	48.1
49	49.1
50	50.1
51	51.1
52	52.1
53	53.1
54	54.1
55	55.1
56	56.1
57	57.1
58	58.1
59	59.1
60	60.1
61	61.1
62	62.1
63	63.1
64	64.1
65	65.1
66	66.1
67	67.1
68	68.1
69	69.1
70	70.1
71	71.1
72	72.1
73	73.1
74	74.1
75	75.1
76	76.1
77	77.1
78	78.1
79	79.1
80	80.1
81	81.1
82	82.1
83	83.1
84	84.1
85	85.1
86	86.1
87	87.1
88	88.1
89	89.1
90	90.1
91	91.1
92	92.1
93	93.1
94	94.1
95	95.1
96	96.1
97	97.1
98	98.1
99	99.1
100	100.1

--

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: _____