MC DATA PROTECTION
Policy at Hurst College and Head Office 2018

Contents:

Background	**What is happening to the data**	**Records Management / Retention**	**Information Security Strategy**
Introduction	The DPO	Paper records	Children's Info
Terms	Records management	Electronic records	Information security
Description	Privileged access	Company devices	Entry controls
Who - Data subjects	Sharing data	Personal devices	Disposal
Why - Purposes	External sharing	Removable media	Breaches
What – Categories	International transfer	Social media	Risk Assessment
Where – Sources		Equipment	
Who we share with		Tracking of paper	
Quality of records			
Summary			
Implement & review			
Privacy Notices			
Consent			
Rights			

Background

Introduction

MC considers itself 'data rich', with lots of electronic storage transmission of data, which is accessible from remote locations, as well as paper records spread over a wide Summer School campus, with potential for loss.
Everyone in the school has the responsibility for handling protected or sensitive data in a safe and secure manner.
This Policy, our Consent Forms (for students and employee) and Privacy Notices were updated 25th May 2018 in line with new GDPR rules. This updated version reflects some new principles, new rights, special attention to children's data and new definitions of and stricter rules on obtaining consent.
The Policy is the result of a Data Protection Impact Assessment.

Terms used

Company name = Manor Courses Limited (Ltd), called MC in the below.
Registered Company in England = No. 1320278
Organisation address = Bishopstone, 36 Crescent Road, Worthing, BN11 1RL
Contact = 8 Dean Court Rd, Brighton, BN2 7DH, UK
Tel = 01273 911377
ICO Registration = No. A8120712

Some terms/acronyms/codes referred to:

- MC = Manor Courses, the company, the Data Controller
- Head Office = 8 Dean Court Rd, Brighton, BN2 7DH, UK
- Summer School = also the company, when our Courses take place at Hurst, for 5 weeks
- Hurst = Hurst College and the campus, College Lane, Hurstpierpoint, West Sussex, BN6 9JS
- Office = summer office at Hurst
- Campus = the grounds, classrooms, facilities, boarding houses at Hurst College
- GDPR = General Data Protection Regulations 2018

MC DATA PROTECTION

People:

- Data Controller = MC
- Directors = the main contacts for MC: Nick (Nicholas) Barnard, Jon (Jonathan) Barnard, Su (Susanna) Barnard
- Data Protection Officer (DPO) = Jon Barnard (Director, Recruitment Officer)
- Customer = Direct Customers: students, parents/guardians. Other: agents and Group Leaders (GL)
- Agent = those companies who send their customers to MC, who collect their own data direct from their customers and share it with us. In many respects they are also Controllers of their data, which they give to us to use for our purposes at Hurst College.
- Employees = more commonly referred to as staff in other MC documents, also includes the Line Managers. In this Policy 'employees' is generally used to refer to their rights and the data we hold on them as 'subjects'. 'Staff' is generally used to refer to them in their duties meeting MC's purposes, their access to and usage of data, and often they are referred to as 'MC staff' to differentiate them from staff of other organisations.
- Students = they are customers, but are also sometimes identified as 'children' to emphasis the fact that as data subjects the risk is higher in terms of safeguarding.

Department / Team Line Managers (LMs) and other acronyms/codes referred to in this Policy:

- English Line Managers (LM) are Director Of Studies (DOS) + Assistant Directors Of Studies (ADOS)
- Activities Line Managers (LM) are the Activity Managers (AM)
- House Line Managers (LM) are Welfare & House Coordinators (WHC) + House Team Leaders (WHC)
- First Aiders (FA)
- Front Office Manager (OM)
- Photographer (CM, Cameraman)
- Welfare Manager (WM)
- Security (SEC) (non-residential, night staff)

For clarification, the below groups signify the usage of different terms for similar meanings, where one word is taken to have very similar meanings to another word:

- records, data, information
- obtain, request, collect *data*
- share, process, use *data*
- access, transfer, transmit, disclose, send, pass, release, receive, return *data*
- hold, retain, store, keep *data*
- dispose, delete, destroy *data*
- recipient, processor
- manual, paper, printed *records*
- digital, electronic, online
- external, third party, outside MC
- malicious, misuse, abuse, unlawful access of *data*
- sensitive, special category, high risk
- server, cloud, Dropbox, Google drive
- equipment, computer, hard-drive
- device, tablet, iPad, removable media
- we believe in MC's case the recipient is the processor because although they don't often change the data, they do access and need it, mostly for registers

Description of data processing

The following is a broad description of the way MC (Data Controller) processes personal information. There is a statutory and contractual obligation for customers and employees to provide some of this information. Other information is obtained by consent.

To understand how customers' or employees' personal information is processed, in addition to this Policy they may also need to: refer to any personal communications they have received; check the Privacy Notices MC has published; or contact MC to ask about their personal circumstances.
The amount of data MC hold is limited, however, it concerns approximately 800 customers and employees ('subjects') who are current, and some of it is held for long periods. It is not excessive for its purpose, but it does include ex-customers/employees. But it could be high risk.
There is no automated decision making at MC.

Who the information is processed about – data subjects

We process personal information about:

- employees (and candidates who do not get recruited)
- customers (students, parents, guardian, agents, GLs)
- professional advisers and consultants
- enquirers

Reasons/purposes for processing information and the lawful/legal bases

We process personal information to enable our legitimate interest as Data Controller, to:

- *provide Residential English Language Courses (education programmes conducted outside the UK State system), in addition to leisure, welfare and support services at our Summer School at Hurst College; maintain our own accounts and records, for administration in connection with boarding and the organisation of our Courses; and to support and manage our staff and students.*

The 4 main lawful bases we rely on to obtain and process this information are:
consent; contract; legitimate interest; vital interests.

for the purposes of..	***in accordance with the legal basis of…***
• provide education, support student learning • monitor and report on attendance/achievement/assessment	Performance of Contract
• social media communication with current audience to: o celebrate the achievements of students o promote to potential parents/agents o engage with student and parent/agent community o share resources/advice	Consent (or parent and/or child)
• provide appropriate medical and pastoral care and welfare support • behavioural information	Performance of Contract, Protection of Vital Interests
• keep children safe, child protection policy • health and safety of all school participants	Protection of Vital Interests
• assess the quality of our services , customer satisfaction • offer correct service	Consent (of child), Legitimate Interest of MC
• select, delegate and support staff • maintain accounts and records	Compliance with Legal Obligation

In addition, concerning any sensitive (special category, high risk) student and employee data regarding:
welfare and mental health, medical information and physical health, dietary requirements, discipline records, information relating to criminal offences or alleged offences
we might also share this information for the purposes and legal bases below.

• keep children safe, child protection policy • provide appropriate medical and pastoral care	Protection of Vital Interests
• select, delegate and support staff	Compliance with Legal Obligation

Type/classes/categories of information processed

We process information relevant to the above reasons/purposes.
Regarding students, parents/guardians, and sometimes group leaders:

- personal identifiers and contacts (such as name, contact details and address)
- parent/guardians' contact details
- characteristics (such as language, age)
- safeguarding information (welfare reports if any, disclosure or allegations made by or against, *if any*)
- mental health, special educational needs (*if any*)
- medical (allergies, medication, dietary requirements, *if any*)
- attendance (excursions, accommodation, sessions attended, absence frequency and reasons)
- assessment and achievement (English class, level placement test results, awards for activities)
- behavioural information (opinions, social-media profiles (including interests), discipline reports, *if any*)
- transport arrangements (to/from airports, or other leisure facilities, *if any*)
- images (photo, video, appearance, behaviour)

Regarding employees:

- personal identifiers and contacts (such as name, contact details and address)
- characteristics (such as language, age)
- mental health (*if any*)
- medical (allergies, medication, dietary requirements, *if any*)
- assessment and achievement (previous employment, qualifications)
- images (photo, video, appearance, behaviour)
- financial details, eg. invoices, salaries, tax, national insurance
- performance records, references, discipline records (*if any*)
- criminal records, vetting checks for employees and GLs

We also process sensitive (special category, high risk) classes of information that may include:

- medical or physical health
- welfare or mental health
- information relating to offences or alleged offences

We do not hold or use/process the following sensitive (special category, high risk) classes of information but it may be assumed from dietary requirements, name, appearance and behaviour:

- race, ethnicity, religion

Where we get the information from - source

We collect student, parent/guardian, employee and GL information via:

- Student enrolment forms – by email, post, online – from parents/guardian
- Agent group registers – by email - from agents
- Staff application forms and application procedures – by email, post, online CV upload

Electronic information may come as attachments or links to online documents/folders. Paper copies may be posted or printed by MC and again photocopied.
Our information may include not only information given to us, but also created/generated by:

- us, MC, the data controller
- MC staff or group leaders (controllers and processors)
- students themselves (children, the data subjects) eg. through questionnaires, participation registers
- external – according to incidences – from eg. NHS, airport/visa security, police

Who the information may be shared with – recipients (or data processors) - and when

We routinely share the personal information we hold amongst MC staff.
We sometimes need to share the personal information we hold amongst other organisations. Where this is necessary we are required to comply with all aspects of GDPR.
Here is a description of the types of organisations we may need to share some of the personal information we process with, for one or more reasons. Only the first in the lust is routine.

Who	When
employees/staff, via team Line Managers	In summer, daily, especially the start and end of each week
agents and GLs	End of the course, if there is any incidence,
suppliers (eg. the Hurst College catering)	Start of summer
examining bodies (eg. when students take a Trinity exam)	If there is any occasion
current, past and prospective employers (eg. recruitment for MC, or references about ex-MC employees)	Post summer (for employee only)
family, associates and representatives of the person whose personal data we are processing	If there is any incidence, in the absence of parent/guardian
financial organisations (eg. accountants)	End of summer contract (for employee only)
central and local government (eg. for tax)	End of summer contract (for employee only)
healthcare professionals, child protection and safeguarding bodies, social and welfare organisations (eg. in cases of injuries or accusations of abuse)	If there is any incidence
police, courts, tribunals and security organisations (eg. in cases of employees or students committing offences or being accused of such)	If there is any incidence
the media (eg. in cases of emergencies or public events)	If there is any incidence
professional advisers and accreditation bodies (eg. British Council (BC))	If there is any occasion (eg. inspections)
service providers at or outside Hurst (ie. activities provided on Hurst for MC by external companies (eg. horse riding school))	If there is any occasion
service providers outside Hurst by transport companies and accommodation (eg. Jade travel for taxis, Canaan Holidays for UK Tours before or after the stay at Hurst)	If there is any occasion

Quality of records

Data is only collected for business purposes. This is kept for stipulated periods of time, dependent on the purpose and department. The same applies to emails sent and received, and any attachments.
We try to record only factual information. However, reports are also made of accusations and the stages of investigations of events.
We will update any inaccurate data if identified to the Directors or Line Managers.
Excessive or irrelevant data is deleted at a period decided between the Directors, not routinely or systematically.

Summary

The Data Protection Officer (DPO) is responsible for making sure MC comply with the GDPR. The DPO is Jon Barnard.
Personal data will **only be used** for the purpose of organising and running the Summer School.
It will **not be shared** with third parties, except those in the list 'Who the information may be shared with' above.
MC:

- tell people **how** we will use it when collecting personal information.
- keep records of people's personal information **up to date and do not keep it longer** than necessary.
- have measures in place to keep the personal data we hold **safe and secure**.
- have a process in place so we can respond to **requests to access** the personal information we hold.

If the information we need/request **is not given**, we may not be able to offer the service in our contracts with the customer or employee. Some extra information is given **by their consent**.
There is no automated decision making.

Implementing and review

This full Policy is distributed to staff during induction and they acknowledge it in their post induction checklist. It can be found on paper in the office.
Staff are not provided data protection training but they receive guidelines within this Policy, and LM are given further opportunities to feedback and adapt them to fit the practicalities of the job.
Customers can read our Policy on the website http://www.manorcourses.co.uk/privacy-policy/.
This Policy is reviewed annually, most recently on 25/5/18, to be implemented from 25/5/18.
An abridged Policy regarding employees' records is in the Staff Handbook.

Privacy notices

Through the website we make this Policy known to all website users and those who submit an online information request form or an enrolment form. Our Privacy Notice and Cookies Policy are at http://www.manorcourses.co.uk/privacy-policy/ .
It provides basic details about what information we collect and why we use it, what happens with it, how we store it, who we share it with. The Notice redirects individuals to read this Policy for further information about where and how information is stored, and how and when it is destroyed.

Consent

This is only one of the lawful bases MC use to obtain information it wants/needs to use.
Parent/guardian receive Consent Forms for their children, group leaders receive it for their groups.
Employees and students both receive abridged versions, and sign them themselves at Hurst.
They aim to be specific, unambiguous, in clear English, asking for affirmative action if they agree, or not, to our holding and using their data, and other requests. There are separate questions for each request we make. Any individual can withdraw their consent by email.

Rights, Freedom of Information, and Access Data/Records Requests

Individuals are allowed to check the records we keep, and to ensure they are up-to-date, and that we are processing their information.
These are their rights:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- have inaccurate personal data rectified, blocked, erased or destroyed
- seek redress, either through the ICO, or through the courts

to check information or use their rights:

- Direct customers, or ex-customers (students, parents/guardians), should email su@manorcourses.co.uk .
- Agents, group leaders, or other enquirers, should email nick@manorcourses.co.uk.
- Employees, or ex-employees, or unsuccessful job candidates, should email jon@manorcourses.co.uk .

We will reply by email within 1 month.
Any request will be coordinated with the DPO (Jon Barnard).
Any requests for specific information about welfare and accommodation or academic performance will be passed to the relevant LM who was involved in processing the information.
LM, WM, OM, FA, and Security will be informed of their expectations in meeting these legal requirements and helping provide the requested data.

What is happening with the information/data?

The DPO – Jon Barnard

MC is registered with the (ICO Information Commissioner's Office), number A8120712.
The DPO audits and manages the staff who process data at the MC level.
The below is all coordinated by the DPO. The DPO will:

- inform all employees of their obligations, as well as monitor the company's (as Data Controller) compliance with the law and Policies.
- determine and take responsibility for the information risk assessment.
- conduct a Data Protection Impact Assessment and ensure Audit Logs are updated
- appoint temporary System Controllers, who are Line Managers that pass information to their team and pass it back to the Directors.

Records management responsibilities

Personal information on employees and candidates is **shared by** Jon Barnard **to** Su Barnard, FA, WM, accountants, British Council, Hurst, agents and relevant LMs.
Personal information on students is **shared by** Nick Barnard **to** Jon Barnard, Su Barnard, relevant LMs, WM, OM, WM, FA, GLs, agents and Hurst.

Methods

Most **post and email communication** to students, parents/guardians and agents is **to/from** Nick Barnard and Su Barnard.
Some information may be **forwarded to** LM.
Most **post and email communication** to employees and prospective candidates is **to/from** Jon Barnard.
Printouts from emails or **photocopies** of document posited may be passed to LM, FA or OM.
Information **shared between** the company departments, or **from** Directors **to** LM, OM, WM, FA or security, is usually **via email, text, Dropbox, the Hurst server, or on paper**, but may also be transferred by **voice on phones and walkie-talkie radios**.
Only the Directors **use removable media devices** within the office at Hurst, during Summer School.
Some information is **passed to** other bodies outside MC, usually **via email**, in instances identified in the list 'Who the information may be shared with' above.

Privileged access, coordinating and monitoring

Privileged **access to data is given to** LMs, OM, WM, FA and security. These are all returnee employees, with suitability references and police checks undertaken.
During summer, LM are responsible for **passing information to** their respective teams digitally (as above) or on paper.

Access

These designated people are **authorised** to create passwords/usernames for log-in accounts for members of their team.
The staff they have **authorised** to access information are **deleted, disabled or blocked** from access after summer by the LM.
Furthermore, LM are **deleted, disabled or blocked** from access after summer by the Directors.
WHC may during summer monitor compliance to see any irregularities in access to data.

Sharing / disclosing data

It is an offence to release customer or employee records without the Directors' consent.
Only in emergencies can employees **give out** information to an external person/organisation.
A controller < > processor contract is assumed after staff have read and acknowledged agreement to this Policy at Induction.

Between staff

Most information about students - including: names, DOB, nationality, agents, arrive and depart dates - is **shared to** the relevant team/employee **from** the Directors **via** the relevant LMs.
All staff are **authorised to share or disclose** student information (except sensitive data) to all other staff of MC: their own and other LMs, members of their team, members of other teams, Directors, FA, WM, OM, security.

Situations that may involve **sharing** student information include: attendance registers and absences; class or house changes; welfare or health concerns; discipline issues.

Externally sharing student information

Information **requested by** Hurst is normally **provided to them only by** the Directors.
Information **requested by** taxi drivers, coach companies, hotels agents, official bodies, local/central government, health and welfare professionals is normally **provided to them only by** the Directors.

Issues regarding staff

Staff **only share** this information with relevant LM or with WM, FA, Directors or security.
Security, WM, FA and Hurst **only share** this information with Directors.
Staff **only share** information regarding LMs with Directors.

External sharing, third parties / suppliers / providers

Only the Directors make decisions on whether or not to share data externally.
However, during emergencies or serious incidences, staff may share personal data with ambulance/health services, criminal/police, welfare professionals or local/central government.
In such instances this will always be reported to the Directors as soon as practically possible.
We may give some data to a number of third parties (providers of services) that have been contracted to assist MC fulfil our business purposes. This is not routinely.
Written agreements are not in place with many providers but they are given this Policy.
External companies that use students' names and ID, such as taxis, are asked to delete data as soon as they no longer need it for their business purposes or after they have sent their invoice to MC.
We will share data on an obvious and appropriate legal basis with official bodies that request it, including police, NHS, child protection bodies. Other bodies that we will share this with include British Council, accountants, transport companies, horse riding schools, insurers, and Hurst College. They all have their own Privacy Notices.

International transferring data (outside EEA/EU)

To an extent, MC does on occasions transfer data to other countries out of EEA/EU.
This only occurs when the Directors' laptop computers are taken abroad, and the laptop contains **digital** information on the **hard drive**.
Staff recruitment is partly done from Japan. The purpose of this is for recruitment decisions and advance deployment of staff to match student needs prior to Summer School opening.
Emails sent to jon@manorcourses.co.uk with attachments may be received, opened, saved and/or printed from staff while in Japan.
Furthermore, **emails** are exchanged containing links to **data and documents** stored and shared between the Directors on Dropbox, these are accessed from abroad. This information could be regarding personal information of students or potential and already recruited employees.
This information is protected via passwords to access the laptop, and information held in the Central Staff Database is protected for access and edit by only Su Barnard.
Paper copies are on occasion transferred out of EEA/EU. This includes printout of staff application forms, qualifications and references. Documents printed outside of EEA/EU will always be moved to UK Head Office each summer for future usage and storage.
As this work is internal, does not involve third parties, MC assesses that the company's protection is adequate for the above transfers. The company mechanisms and internal working systems provide the necessary security precautions to the same level as if the laptops and paperwork were in UK/EEA.

Records Management / Retention

Paper/manual records

Usage

Registers normally hold only name, gender, nationality and age, plus their house/bedroom, or classroom/level. Sensitive medical/health data may appear on some registers to protect vital interests, especially in houses.

Printed *class registers* are **given by** DOS **to** teachers at the start of each week, or teachers may print these themselves from digital registers. They may make edits/updates in pen and transfer that information back to DOS at the end of each week.

Printed *house registers* are **given by** WHC **to** respective house managers each week, or house managers may print these themselves from digital registers. They may make edits/updates in pen and transfer that information back to WHC at the end of each week.

Printed *excursion group registers* are **given by** OM **to** staff and GLs accompanying MC Group students on excursions.

Printed *activity/quad registers* are **given by** OM **to** GLs and MC Group Leaders. GLs in fact already hold this information already, and are assumed to also be Data Controllers of the students in their group.

Printed *medical registers* are **printed by** FA with sensitive data including medical issues. They do not give them to anyone but may pass on some information where relevant.

Information is **adapted** into *medical reports*, and vice versa, *medical report/incident* information may be **transferred** into the *register/database*, **input by** FA or Directors.

Printed *progress reports* for students are handed to the student, but saved on the server.

Hand-written paper *free-time* and *activity attendance registers* **by** students themselves are **kept by** campus patrollers and ALs and **filed** at the end of each session (for free-time) and day (for activities).

Hand-written paper *discipline, welfare, absence reports* for students or employees are **written by** WM.

Hand-written paper *absence reports* for students are **completed by** ADOS, GL, and/or FA.

Storage

All paper lists will be **returned to** the relevant LM or office, **not discarded**:

- class registers - **filed** in the relevant class folder, **returned to** the ELT Resources Room at the end of each teaching day, **kept** there until the end of Summer School
- house registers - **filed** in the relevant house folder, in a bag, **returned to** House office daily, **kept** there until the end of Summer School
- excursion registers - **returned** to and **filed at** the office after excursions, **kept** there until the end of Summer School
- activity/quad registers and reports - **filed** in the office after each registration period, **kept** there until the end of Summer School
- medical records - **handed** to WM at end of Summer School, **returned** to Head Office after Summer School
- progress reports for students - **handed** to the student, but **saved** on the server
- activity and free-time registers - **hand-written by** the students, **filed by** AM and OM respectively, **kept** in office until the end of Summer School
- hand-written *discipline, welfare, absence reports* - **filed by** WM in the office, **returned** to Head Office after Summer School
- hand-written *absence reports* - **kept** in the office, and once completed **filed** in the ELT Resources Room **by** the ADOS, **kept** there until the end of Summer School

Deletion

Some above papers are **destroyed securely by shredding** at the end of the Summer School **by** respective LM, or OM on the Hurst campus.

Some are **destroyed securely by** shredding **by** Directors **at** Head Office within a month of Summer School closing.

Welfare concerns (including discipline, allegations, safeguarding and 'prevent') reports about both employee and students are **stored securely** in the Head Office after Summer School.

Compliance and monitoring

Duty checklists remind employees daily to **file** paper registers only in specific locations and **not to discard** them themselves.
After LMs and OM **destroy** the paper records they complete a 'Destruction Log' and **sign** a 'close of Summer School' sheet at the end of their contract.

Electronic records

A range of records and other data are **stored on** basic versions of a central database on Dropbox or similar **accessed from** MC devices/tablets or Hurst computers.
Other data may be **stored on** the Hurst server but only accessed by Hurst computers.
There are a range of facilities to store and share data, but additionally walkie-talkie radios are used to transfer it but not store it.
See below.

Company devices

Tablets/iPad/devices are allocated during induction to HM. HM keep the usage guidelines in house bags for OTHER staff who access the device.
These have individual codes/PINs for each device.
Most data is backed-up on and/or accessed from a server/Dropbox.
Security software/apps are installed.

Usage

Staff **use** devices all over the campus, but they are **not permitted** off campus.
Staff will:

- **not take off** campus or **use** them in public places due to physical risks, such as loss or theft, and insecure Wi-Fi networks or other people watching them.
- **rely on** paper registers and checklists off campus.
- **not input** student names into staffs' personal phones or devices, but if the numbers have been used on phones then the contact name **must not be saved**.
- **return** paper lists with phone numbers **to** the office.
- **not use email** or download things for personal purposes to company devices, and when doing so for company purposes, to **ask** the LM.
- **log off** or l**ock** devices and computers when they finish.

Passwords are **changed** annually.

Personal devices

We do not permit most staff to use their own equipment for the storage or sharing or accessing or usage of MC data. Personal devices are not checked for similar standard of security.
However, LM, FA, WM and OM may use their own personal equipment.

Usage

If used for work purposes, staff will:

- **inform** their LM.
- **not collect** information for non-business purposes.
- **delete** all student data from their personal devices after it has been used for its business purpose.
- **collect** Student phone numbers **on** paper for the duration of an excursion, and **not input** into phone contacts.
- **delete** numbers from their phones after every excursion.
- Phone calls made or received **may remain** in the memory of the phone but if they are **named** as a contact, they will be **deleted** at the end of the excursion.
- **sign** a 'close of Summer School' sheet as a 'Destruction Log'.

Home working

When personal devices are taken off campus during staffs' time off, it will **not carry** any data.
Staff will **not be expected to carry out** any work for MC, unless **authorised** with the Directors.

Removable media, MC or personal

Data may **not be transferred** to locations around the campus via USB, which may be the personal property of staff.

Sometimes however, in the failure of other equipment, this may be the easiest method of transfer/storage.

Usage

If used for work purposes, staff will:

- **delete** data.
- **not leave** removable media unattended.
- **report** any instances of theft or loss.

The CM logs photos and **saves onto** an MC hard drive regularly.
These photos rarely carry information about the students/subjects' name.
When off-campus the CM **carries** removable memory discs which **store** photos.

Social media

Staff will abide by our Staff Social Media Usage Policy and remain aware of our Official MC Social Media Policy. Parents/guardian and GLs should read these Policies and make their children aware.
Names and identities of students can **also be accessed** via social networks. These profiles are **administered and accessed by authorised** staff, OM, CM and WHC. Passwords are **changed** annually.
Users with admin access are **removed** from accounts at the end of each summer.

Equipment

MC equipment

Existing and all new equipment is **configured** to reduce vulnerabilities by our technical support company.
Anti-malware defences **protect** hardware.
Personal devices are **not checked** for similar standard of security.

Hurst equipment

These **can be used** for staffs' personal purposes.
Staff will:

- **be careful** when **using** them for personal purposes, **opening attachments and downloading**.
- **log off or lock** devices and computers when they finish.

Software, programmes, sites or downloads can be **requested for unblocking** via a form in the front office, which will be passed to Hurst IT for them to assess and permit. The same applies to phone apps.

Tracking and recording the movement of manual/paper records

At Hurst during summer

Paper records at the Hurst campus are either **kept** in the office, classroom block or houses.
Records in the form of registers are also **temporarily kept** at the place of activities, but **filed** daily in the class block or office.
The only **securely kept** records are confidential ones. Welfare concern records/reports, allegations, staff discipline and Police/criminal checks are **locked securely** in the office throughout summer school. The secure storage (lockable cabinet) is in a locked room within the office.
Health records are **locked up** in the FA office overnight.
In general, paper copies are **moved between** houses to office or classroom block in authorised and identified company bags or clipboards, usually **by** duty staff in uniform.
CCTV **records** instances of paper records being **removed or amended** without authorisation from the office.
Employees' names and phone numbers are **carried on** excursions and **between** Hurst and airports.
All paper copies of these lists are **returned** to the office upon return after the duty.

Away from Hurst, after and before summer

throughout the year, those records that have been **kept** for a longer period are at Head Office.
Electronic records on laptops are **transferred** abroad at certain times through the year, solely for the purposes of continuing the business while the Directors are abroad (eg. resident in Japan). Paper copies **rarely accompany** them.
Head Office and its cabinets are **secured** with keys.
During **transit** between Hurst and Head Office paper records are **carried in person** by car with the Directors.

Information Security Strategy

Children's Information

Although much of our data is not sensitive, because it refers to customers (children) in an obvious location, which is physically accessible by adults from within and outside MC, there is a high risk that access to data combined with physical or online access to children is a major child protection concern. Furthermore, recent GDPR reminds staff of their role in child protection because children are less aware of the risks.
In recognition of this, MC and staff have the obligation to also protect students' identity from theft via loss of their digital/electronic equipment. This is done by securing the houses from intruders, but not the bedrooms from other students. CCTV can be viewed but cannot access all areas. Students are therefore recommended to lock their valuable items in their suitcases or keep them in the office with their ID/passports.

Information security at Head Office and Hurst

Hurst IT department and MC's technical support provider advise and implement security measures at Hurst and Head Office respectively.
Back-ups take place regularly at Head Office only, out of summer season.
Security of paper records and their movement and disposal is outlined below.
Digital data includes a wider range of information and is held in a larger number of locations (amount of devices, and range of locations they are kept and used). Disposal procedures and standards are therefore more complex.

Entry controls and physical access to Hurst premises

Codes, swipes, keys, ID

Hurst **reassigns** new codes or swipe cards for MC at the start of summer.
This enables MC or Hurst to **track who has accessed** where and when.
Staff **acknowledge** the code of conduct for usage, and **return** them at the end of summer.
Staffs and GL **carry** MC ID name badges with photos.
Students **sign** themselves into and out of houses in pen.
Hurst provides staff to **lock up** at night and unlock non-residential buildings in the morning.
Hurst cooperates when MC request to **view** CCTV.
Staff bedrooms have keys, but students' bedrooms do not.

Office

No staff have **access** to the office when the Directors lock it, except security.
The office, where records are not locked, is **accessed** via codes shared between LMs, FA, WM, OM, security and Hurst personnel. The door that uses codes does not recognise who entered or when.
The secure storage is a **lockable** cabinet in a **locked** room within the office. Keys are **restricted to** Directors, OM and WM only. A paper folder **records who accessed** it and **withdrew and returned** records (including passports).

Records, devices when not in use

During excursions, devices are **kept** for long periods in the class block, but they are **locked by codes**.
Paper records of house, activity and class registers **remain** in their designated locations in the classroom block throughout the summer course. These buildings are on codes/swipes for most of the day, except periods to give students free access, and **locked** by Hurst overnight, but the classrooms are **not**.

Visitors to the campus and security

Visitors are **signed in and out** of campus, and given ID, when they visit the campus at the office.
They are accompanied round campus as much as is possible by their host.

Records / data disposal / destruction by Directors

Data is **not kept** for longer than necessary for its purpose. We **attempt to delete** records within set periods, and maintain a 'Destruction Log'.

Electronic

Deletion does **not** always mean the record has been **destroyed** because it **may still exist** in MC's systems. In cases where it is **not absolute**, and has **not fully been destroyed**, some electronic versions **may be kept** but with **no intention to use or access** it again. Cases where this may happen

include when reference is made to employees or customers in a batch of other information that is not yet intended for deletion. Such information is **never stored** for the purpose of giving it to another organisation
Email communication is **archived and kept indefinitely**, until a customer or an ex-employee or unsuccessful candidate requests their deletion in line with their rights.
Paper
Paper records of employees are **kept** from 1 year after they begin their contract, thus it covers the period during recruitment too, and therefore extends over a year. If employees re-apply and are successful in gaining a contract the following years, the period through which we **keep** these records will then **extend** another year, and so on.
Candidates who are not offered or did not accept a contract will be **disposed** of within 9 months.
Paper records are **destroyed securely** with a shredder at the Head Office.
After Summer School closes, LM will **box** any undestroyed student records into one box in the Hurst office to be **transported** back to Brighton/Head Office. This will be **shredded** within a month.
Welfare, behaviour, discipline and health reports and concerns are **kept** on paper until the following summer, for a 1 year period in case situations that occurred at Hurst develop when the student or employees returns home. Allegations, accusations and disclosures will be kept for longer.
LM are never responsible for disposal of employee records.

Breaches

MC forbids unauthorised disclosure, modification, removal or destruction of data.
However, conscious theft, malicious use or unlawful processing may occur.
Furthermore, deletion, transmission, loss, damage copying or viewing may occur by mistake, or equipment may fail or degrade.
It will not be obvious if any unauthorised person has accessed this information, so measures have been taken to keep this as secure as is practically possible, and as limited in quantity as possible.
Obvious incidences include loss of a laptop or device, missing papers, irregular log-in/access times/locations. All instances will be investigated.
Responses and measures taken in instances of a breach of this security depend on whether any information has been accessed, and any action has been unlawfully taken and how the data has been misused.
Employees will report breaches to the Directors, who in turn will record, then report to ICO within 72 hours, and follow advice. The Directors will begin investigations and implement recovery plans if necessary.

Business Impact Analysis, Information Risk Assessment

MC wishes to put no individuals at risk by its holding of their information.
Assessed against the criteria of: *confidentiality; integrity; availability,* we consider the risk of losing or having our data misused, is low.
Confidentiality:
The greatest risk to information being unlawfully accessed will be in Confidentiality.
For example child protection concerns surrounding a breach whereby somebody from within or outside of MC found the identity, behaviour patterns, images and/or location of a child.
Regarding employee data, access to the most sensitive information about discipline or performance records at Hurst/MC, or criminal records from prior to MC, would raise reputational concerns for those employees, and loss of trust in the employer.
Integrity:
If information was changed mistakenly or wilfully, the greatest impact will be logistically. Confusion may be caused to staff duties, but no danger posed. Higher risk would be in medical areas, where accurate records are necessary, mistakes in that information could be critical.
Availability:
On campus, the same information is usually available from different sources, however, loss of paper records that were not yet stored digitally would impact us logistically. Confusion may be caused to staff duties, but no danger posed.
Off campus, the loss of paper or digital records accompanying staff and students could be critical to the children health and safety.
In any instances of the above the DPO will plan for:

- *communications; non-reoccurrence; further awareness raising.*