‘MC DATA PROTECTION Policy’ at Hurst College and Brighton Office/s 2023

Contents:

This Data Protection is linked to in the Welfare Page of our website.

Background

Introduction

MC considers itself ‘data rich’. There are lots of electronic storage transmission of data, which is accessible from remote locations, as well as paper records used over a wide Summer School (Hurst) campus and transferred physically between the campus and the Brighton offices. Therefore there is 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 in 2018 in line with GDPR rules, and again in 2023. This updated version reflects principles, rights, definitions, special attention to children’s data and stricter rules on obtaining consent.
The Policy is the result of a Data Protection Impact Assessment in 2019.

MC DATA PROTECTION

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 = 67 Warren Way, Brighton, BN2 6PH, UK
Other office addresses as of April 2023: 18 Chapel Mews, Brighton, BN3 1AR, UK
ICO Registration = No. A8120712
MC uses a law firm in EU designated according to Article 27 of GDPR.
EU-GDPR representative acting on behalf of MC = Rickert Rechtsanwaltsgesellschaft mbH, Germany.

Some terms/acronyms/codes referred to:

- MC = Manor Courses, the company, the Data Controller
- 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
- Brighton Office/s as of April 2023 = 67 Warren Way, Brighton, BN2 6PH, UK and 18 Chapel Mews, Brighton, BN3 1AR, UK
- Office = summer office at Hurst, used by the Directors, FA, OM and WM
- Campus = the grounds, classrooms, facilities, boarding houses at Hurst College
- GDPR = General Data Protection Regulations

EU regulations - MC uses a law firm in Germany designated according to Article 27 of GDPR. Enquiries from EU citizens/companies about MC's data should contact our EU-GDPR representative:

- Rickert Rechtsanwaltsgesellschaft mbH, Manor Courses Ltd,
  Colmantstraße 15, 53115 Bonn, Germany
  art-27-rep-manorcourses@rickert.law

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.

MC DATA PROTECTION

MC Staff are often the Processors, or Sub-Processors. The main Department Staff and Team Line Managers (LM) 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), sometimes is a LM or OM
- Welfare Manager (WM)
- Security (SEC) (non-residential, night staff)

For clarification, the below groupings contain words that are roughly the same. This is to signify the different usages by MC (in our various policies and documents) and GDPR law etc. 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
- shared drives, server, cloud, iCloud, OneDrive, Dropbox, Google drive
- laptop, computer, PC, hard-drive
- equipment, computer, hard-drive
- device, tablet, iPad
- smartphone, iPhone, Android
- removable media, USB, flash drive, memory stick
- subjects include: staff, employee, teacher, leader
- subjects include: client, customer, agent, parent, child, student

We believe in MC's case the *recipient* (various MC staff) 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 previous personal communications they have *received*;
- check the Privacy Policy & Cookies Notices MC has *published* *https://www.manorcourses.co.uk/privacy-policy/* ;
- or *email* MC info@manorcourses.co.uk to ask about their individual circumstances ;
- or EU citizens can contact art-27-rep-manorcourses@rickert.law

MC DATA PROTECTION

The amount of data MC hold is limited, however, it concerns approximately 1000 current/ongoing /upcoming customers and employees ('subjects') as well as those from previous summer/courses/contracts, and some of it is held for long periods.
It is not excessive for its purpose, but it does include ex-customers/employees. 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 - current, ongoing, upcoming, previous
- potential employees, applicants and candidates who do not get recruited
- customers (students, parents, guardian, agents, GLs) - current, ongoing, upcoming, previous
- potential customers, enquirers who contact MC through various communication methods
- professional advisers, industrial bodies, service providers and consultants

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 Protection of Vital Interests
• social media communication with current audience to: ○ celebrate the achievements of students ○ promote to potential parents/agents ○ engage with student and parent/agent community ○ share resources/advice	Consent (or parent and/or child)
• provide appropriate medical and pastoral care and welfare support • behavioural information	Performance of Contract,
• 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/immigration/visa security, police
- external – supplied to us as part of procedures – eg. payroll information from accountants or HMRC

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 list 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, security organisations (eg. in cases of employees or students committing or being accused of offences)	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	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, and may include opinions or interpretations.
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.

MC DATA PROTECTION

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.
- Have an EU representative to deal with enquiries in/from EU.

If the information we need/request **is not given** to us, 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 Privacy Policy & Cookies Notice on the website http://www.manorcourses.co.uk/privacy-policy/.
An abridged Policy regarding employees' records is in the Staff Handbook.

Privacy notices

Through the website we make this Policy available to all website users, which includes those who submit an online information request form or an enrolment form or upload any documents and submit details for job applications.
Our Privacy and Cookies Policy is in the Appendix and 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 Policy redirects individuals to read another Policy for further information about where and how information is stored, and how and when it is destroyed, at https://www.manorcourses.co.uk/wp-content/uploads/2018/06/Privacy-Notice-for-students-MC-at-Hurst-College.pdf
This Data Protection is linked to in the Welfare Page of our website.

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 an abridged version, and sign it themselves at Hurst.
These Consent Forms 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 info@manorcourses.co.uk.
- Employees, or ex-employees, or unsuccessful job candidates, should email jon@manorcourses.co.uk .

Requests from EU based clients and other subjects, should contact our law firm based in EU, in Germany:

- Rickert Rechtsanwaltsgesellschaft mbH, Manor Courses Ltd,
  Colmantstraße 15, 53115 Bonn, Germany
  art-27-rep-manorcourses@rickert.law
- They will liaise with MC and the DPO.

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.

MC DATA PROTECTION

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 LM.

Personal information on students is …

- **shared by** Nick Barnard
- **to** Jon Barnard, Su Barnard, relevant LM, 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 digitally or on paper.
Most **email communication** to employees and prospective candidates is **to/from** Jon Barnard.
Printouts from emails posted 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, iPads/devices/tablets 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 or access to shared drives via log-ins**, 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** LM, 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.

MC DATA PROTECTION

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 LM.
All staff are **authorised to share or disclose** student information (except sensitive data) to all other staff of MC: their own and other LM, 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 performance

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 LM with Directors.

External sharing, third parties / suppliers / providers

Only the Directors make decisions on whether or not to share data externally.
It may happen in the following situations with the following recipients.
They all have their own Privacy Notices.

Unpredicted incidences

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 will share data on an obvious and appropriate legal basis with official bodies that request it, including police, NHS, child protection bodies.

Providers of regular services

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 done routinely.
Written agreements are not in place with many providers but they are given this Policy by email.
External companies that use students' names and ID, such as taxis, must delete data as soon as they no longer need it for their business purposes or after they have sent their invoice to MC.
Other bodies that we will share this with include British Council, accountants, transport companies, horse riding schools, insurers, and Hurst College.
Our social media creators and management company, who also design and maintain our website, also access student data, especially photos and videos.

MC DATA PROTECTION

International transferring data

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, selection, delegation and deployment 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.
A laptop and removable storage devices carrying these, and some paper copies are physically transferred to UK in May and back to Japan in August (before and after Summer School).
Furthermore, **emails** are exchanged containing links to **data and documents** stored and shared between the Directors on Dropbox/OneDrive/iCloud 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 which are emailed to Jon Barnard while in Japan. 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.

MC DATA PROTECTION

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 LM 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.

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.
In the classblock, ET resources and files are in a room on a coded entry system that MC and Hurst personnel can access. HM and AL files are in a room that is accessible by the coded door to the classblock, which may also be accessible by students.
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 might **record** instances of paper records being **removed or amended** without authorisation from the office, but there are blind spots where footage cannot be taken.
Employees' names and phone number paper lists 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 MC's year-round Brighton Office/s.
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** Directors from UK to abroad, but might be accrued from abroad to UK..
Head Office and its cabinets are **secured** with keys.
During **transit** between Hurst and Brighton Office/s paper records are **carried in person** by car or public transport with the Directors.

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.

MC DATA PROTECTION

MC's 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/OneDrive/iCloud.
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.

Other Equipment

MC equipment

Existing and all new IT/digital/computer equipment is **configured** to reduce vulnerabilities by our technical support company.
Anti-malware defences **protect** hardware.
Staff's personal devices are **not checked** for similar standard of security.

Hurst equipment

These **can be used** for staffs' personal and work 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.

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, all other 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, must **not carry** any data.
Staff will **not be expected to carry out** any work for MC, unless **authorised** with the Directors.
However, FA, OM and LM might keep data on personal devices during these periods.

Removable media, MC's or staff's personal USB, memory sticks, flash drives etc.

Data must **not be transferred** to locations around the campus via USB, if it is the personal property of staff, without permission from the Directors or LM. They can borrow an MC USB or memory stick.
FA, OM and LM might keep data on personal devices during these periods
Sometimes, 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 a designated CM **carries** removable memory drive/stick/discs which **store** photos.

Social media, online only data

Most social media is created and managed by an external provider, www.Joojoocreative.com
Staff will abide by our Staff Social Media Usage Policy and remain aware of our MC Social Media Policy. Parents/guardian and GLs should read these Policies and make their children aware. These Policies are found within the "Safeguarding Children and Child Protection Policy, including other related Duty of Care Policies". They are found under the section 'related to Data Protection Policy & Staff IT Acceptable Usage Policy.
https://www.manorcourses.co.uk/wp-content/uploads/2018/06/MC-Policies-2018.pdf
Names and identities of students can **also be accessed** via social networks on MC's accounts/profiles on Facebook and Instagram and our website's blog.
These profiles are **administered and accessed by authorised** staff, OM, CM and WHC.
Users with admin access are **removed** from accounts at the end of each summer. Only limited LM and OM have log-in access.

MC DATA PROTECTION

Information Security Strategy

Children's Information

Much of our data is not sensitive. However, 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, we remind 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 Brighton Office/s and Hurst

Hurst IT department and MC's technical support provider (Alex IT Solutions) advise and implement security measures at Hurst and our Office/s respectively.
Back-ups take place regularly at our Office/s 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.

Hurst 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 LM, 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).
Each department of LM and staff have an office in the classblock. Not all rooms are on codes, but the block/building is on a code, which students may sometimes know (because it gives access to toilets).

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
All visitors to MC, MC's students or MC's staff are **signed in and out** of campus, and given ID lanyards, when they visit us, at our office. Some visitors to Hurst are **signed in and out** of campus, and given ID, when they visit the campus, at the Hurst Reception.
They are accompanied round campus as much as is possible by their host.
There are visitors who enter campus when Hurst Reception is closed, for a variety of purposes and with access to various facilities.
To know which visitors are authorised, MC can consult a Bookings/Lettings Sheet from Hurst with dates, times, locations and users.

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, but do not maintain a 'Destruction Log' outside of summer period.

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 Brighton Office/s.
After Summer School closes, LM will **box** any undestroyed student records into one box in the Hurst office to be **transported** back to Brighton Office/s. 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 employee 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 as soon as we are made aware of them.

Responses and measures taken in instances of a breach of this security depend on whether we know any information has been accessed, and any action has been unlawfully taken and how the data has been misused.
Employees will report breaches they are aware of 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's health and safety.
In any instances of the above the DPO will plan for:

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

APPENDIX 1 - Understanding our Privacy and Cookies Policy

For users of and visitors to our website and social media

Understanding our Privacy and Cookies Policy

This privacy and cookie policy is for www.manorcourses.co.uk and governs the privacy of those who choose to use it and how cookies are used on this site.
The policy sets out the different areas where user privacy is concerned and outlines the obligations & requirements of the users, the website and website owners. Furthermore the way this website processes, stores and protects user data and information will also be detailed within this policy.
There is a separate Privacy Notice regarding other information about students collected by Manor Courses before and during summer.

The Website

This website and its owners take a proactive approach to user privacy and ensure the necessary steps are taken to protect the privacy of its users throughout their visiting experience. This website complies to all UK national laws and requirements for user privacy.

Use of Cookies

This website uses cookies to better the users experience while visiting the website. Where applicable this website uses a cookie control system allowing the user on their first visit to the website to allow or disallow the use of cookies on their computer / device. This complies with recent legislation requirements for websites to obtain explicit consent from users before leaving behind or reading files such as cookies on a user's computer / device.
Cookies are small files saved to the user's computer's hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website.
Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.
This website uses tracking software to monitor its visitors to better understand how they use it. This software is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information. You can read Google's privacy policy here for further information http://www.google.com/policies/privacy/.
Other cookies may be stored to your computer's hard drive by external vendors when this website uses referral programs, sponsored links or adverts. Such cookies are used for conversion and referral tracking and typically expire after 30 days, though some may take longer. No personal information is stored, saved or collected.
However, you may prefer to disable cookies on this site and on others. The most effective way to do this is to disable cookies in your browser. We suggest consulting the

Help section of your browser or taking a look at the About Cookies website which offers guidance for all modern browsers.

Contact & Communication

Users contacting this website and/or its owners do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use, as detailed in the Data Protection Act 1998. Every effort has been made to ensure a safe and secure form to email submission process but advise users using such form to email processes that they do so at their own risk.

This website and its owners use any information submitted to provide you with further information about the products / services they offer or to assist you in answering any questions or queries you may have submitted. This includes using your details to subscribe you to any email newsletter program the website operates but only if this was made clear to you and your express permission was granted when submitting any form to email process. Or whereby you the consumer have previously purchased from or enquired about purchasing from the company a product or service that the email newsletter relates to. This is by no means an entire list of your user rights in regard to receiving email marketing material. Your details are not passed on to any third parties.

Email Newsletter

This website operates an email newsletter program, used to inform subscribers about products and services supplied by this website. Users can subscribe through an online automated process should they wish to do so but do so at their own discretion. Some subscriptions may be manually processed through prior written agreement with the user.

Subscriptions are taken in compliance with UK Spam Laws detailed in the Privacy and Electronic Communications Regulations 2003. All personal details relating to subscriptions are held securely and in accordance with the Data Protection Act 1998. No personal details are passed on to third parties nor shared with companies / people outside of the company that operates this website. Under the Data Protection Act 1998 you may request a copy of personal information held about you by this website's email newsletter program. A small fee will be payable. If you would like a copy of the information held on you please write to the business address at the bottom of this policy.

Email marketing campaigns published by this website or its owners may contain tracking facilities within the actual email. Subscriber activity is tracked and stored in a database for future analysis and evaluation. Such tracked activity may include; the opening of emails, forwarding of emails, the clicking of links within the email content, times, dates and frequency of activity.

This information is used to refine future email campaigns and supply the user with more relevant content based around their activity.

In compliance with UK Spam Laws and the Privacy and Electronic Communications Regulations 2003 subscribers are given the opportunity to unsubscribe at any time through an automated system. This process is detailed at the footer of each email campaign. If an automated unsubscription system is unavailable clear instructions on how to unsubscribe will by detailed instead.

External Links

Although this website only looks to include quality, safe and relevant external links, users are advised adopt a policy of caution before clicking any external web links mentioned throughout this website.

The owners of this website cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note they click on external links at their own risk and this website and its owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Adverts and Sponsored Links

This website may contain sponsored links and adverts. These will typically be served through our advertising partners, to whom may have detailed privacy policies relating directly to the adverts they serve.

Clicking on any such adverts will send you to the advertisers website through a referral program which may use cookies and will track the number of referrals sent from this website. This may include the use of cookies which may in turn be saved on your computer's hard drive. Users should therefore note they click on sponsored external links at their own risk and this website and its owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Social Media Platforms

Communication, engagement and actions taken through external social media platforms that this website and its owners participate on are custom to the terms and conditions as well as the privacy policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate / engage upon them with due care and caution in regard to their own privacy and personal details. This website nor its owners will ever ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through primary communication channels such as by telephone or email.

This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track and save your request to share a web page respectively through your social media platform account.

Shortened Links in Social Media

This website and its owners through their social media platform accounts may share web links to relevant web pages. By default some social media platforms shorten lengthy URLs.

Users are advised to take caution and good judgement before clicking any shortened URLs published on social media platforms by this website and its owners. Despite the best efforts to ensure only genuine URLs are published many social media platforms are prone to spam and hacking and therefore this website and its owners cannot be held liable for any damages or implications caused by visiting any shortened links.

APPENDIX 2 - Privacy Notice - How We Use Student Information

For students (and some parent/guardians) who enroll and join during Summer at Hurst College.

Privacy Notice

How we use student (and some parent/guardian) information received and processed during Summer at Hurst College.
This is separate to our 'Understanding our Privacy and Cookies Policy'

Manor Courses, the company, the Data Controller

Company name = Manor Courses Limited (Ltd), called MC in the below.
Contact = 67 Warren Way, Brighton, BN2 6PH, UK ;
Email = info@manorcourses.co.uk ;
ICO Registration = No. A8120712
Data Protection Officer (DPO) = Jon Barnard (Course Director)
jon@manorcourses.co.uk

The categories of student information that we process include:

- 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*)
- 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)

This list is not exhaustive, but it is the routine collection of data every summer (and pre-summer) period. Other information may be collected by teachers in classes.

Why we collect and use student (and some parent/guardian) (data subject) information

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.*

MC DATA PROTECTION

We collect and use student information, for various purposes. Under the General Data Protection Regulation (GDPR), there are various lawful bases we rely on for processing student information.

for the purposes of….	*in accordance with the legal basis of.....*
• support student learning, provide education • monitor and report on attendance/achievement/assessment	Performance of Contract

• social media communication with current audience to:
  ○ celebrate the achievements of students
  ○ promote to potential parents/agents
  ○ engage with student and parent/agent community
  ○ 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) 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 pastoral care and welfare support services	Compliance with Legal Obligation

MC DATA PROTECTION

How we collect student information

We collect student information via:

- Student enrolment forms – by email, post, online – from parents/guardian
- Agent group registers – by email - from agents/group leaders
- Generated at Hurst College - by students or staff – through questionnaires, participation registers
- External sources – according to incidences – from eg. NHS, airport/visa security, police Student data is essential for the MC's operational use. Whilst the majority of student information you (parents/guardians, or agents/group leaders) provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this (please consult our Consent Form for the latter). You have the right to withdraw any Consent you have given us.

If you do not supply any information we request, we may not be able to offer our full services.

How we store student data

We hold student data securely for the set amount of time shown in our data retention schedule (part of our Audit of Regular Processing, and outlined in our Data Protection Policy). For more information on our data retention schedule and how we keep your data safe, please email the Course Director (also the Data Protection Officer) jon@manorcourses.co.uk or see our Data Protection Policy on www.manorcourses.co.uk/welfare

We outline where data is held, the security arrangements, and policies about safe use of data by staff. Between MC staff and the Data Controller (MC Directors), information is shared electronically. Information generated at Hurst College during summer is shared on paper and electronically.

There is no automated decision making.

Who (recipients) we share student information with

Outside of MC Staff at Hurst College, we do not routinely share student information with anyone. However, in certain circumstance MC may be obliged to share it with:

- Catering and health and safety staff at Hurst College
- External third parties might include our accountants, insurers, industry bodies (eg. British Council)
- Transport companies
- Legal organisations such as NHS (for health), police, or child protection agencies

MC DATA PROTECTION

Why we regularly share student information

We do not regularly share information about our students with anyone without consent unless the law and our policies allow us to do so.
It might be shared for the purposes of: *maintain accounts and records, keep children safe, provide appropriate pastoral care, supply welfare support services.*
Such information is shared on paper and electronically by email with any of the above.

Your rights, requesting access to your personal data

Under data protection legislation, parents/guardians and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational and/or welfare record, contact the course Director (also the Data Protection Officer) jon@manorcourses.co.uk . You have the right to withdraw any Consent you have given us.
You also have the right to:

- 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; and
- a right to seek redress, or lodge a complaint, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance, or if in UK our outside EU, directly to the Information Commissioner's Office at https://ico.org.uk/concerns/
Enquiries from EU citizens/companies about MC's data should contact our EU-GDPR representative:

- Rickert Rechtsanwaltsgesellschaft mbH, Manor Courses Ltd, Colmantstraße 15, 53115 Bonn, Germany art-27-rep-manorcourses@rickert.law

Contact

If you would like to discuss anything in this privacy notice, please contact Jon Barnard, the Course Director (also the Data Protection Officer) jon@manorcourses.co.uk .
If children or parents wish to withdraw any Consent you have given us, email Su Barnard (Director) su@manorcourses.co.uk .
Enquiries from EU citizens/companies about MC's data should contact our EU-GDPR representative:

- Rickert Rechtsanwaltsgesellschaft mbH, Manor Courses Ltd, Colmantstraße 15, 53115 Bonn, Germany art-27-rep-manorcourses@rickert.law

APPENDIX 3 - IT/Data/Devices/Computer/Internet/Media/ Equipment/Systems/Software Acceptable Usage Policy

For staff

This Policy covers the security and use of all MC's and Hurst's information and IT equipment and systems.
It also includes the use of email, internet, voice and mobile IT equipment.
It applies to all information, in whatever form, relating to MC's business activities.
It applies to all MC's employees.
It applied to during working hours for both professional and personal use, and outside working hours while using the systems for both professional and personal sue.

Computer Access Control – Individual's Responsibility

Access to the MC/Hurst IT systems is controlled by the use of User IDs and passwords.
All User IDs and passwords are uniquely assigned to named employees and consequently employees are accountable for all actions on the IT systems.
Employees must not:

1. Allow anyone else to use any given user ID and password.
2. Leave their user accounts logged in at an unattended and unlocked computer.
3. Use someone else's user ID and password.
4. Leave their password unprotected, for example writing it down.
5. Perform any unauthorised changes to MC's and Hurst's IT systems or information.
6. Attempt to access MC data that they are not authorised to use or access.
7. Store MC data on any non-authorised equipment.
8. Give or transfer MC data or software to any person or organisation (outside MC) without the authority of MC.

Internet and Email - Conditions of Use

Professional use of personal equipment is accepted during working hours.
Personal use of Hurst/MC IT systems outside of working hours is permitted where such use does not affect the individual's business performance, is not detrimental to MC in any way, not in breach of any term and condition of employment and does not place the individual or MC or Hurst in breach of statutory or other legal obligations.
All employees are accountable for their actions on the internet and email systems.
While accessing MC/Hurst IT systems during outside or within working hours, employees must not:

1. Use the internet or email for the purposes of harassment or abuse.
2. Use profanity, obscenities, or derogatory remarks in communications.
3. Access, download, send or receive any data including images, which can be considered offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
4. Place any information on the Internet that relates to MC, alter any information about it, or express any opinion about MC, unless they are specifically authorised to do this.
5. Send unprotected sensitive or confidential information externally.

6. Make official commitments through the internet or email on behalf of MC unless authorised to do so.
7. Download copyrighted material such as music media files, film and video files (not an exhaustive list) without appropriate approval.
8. In any way infringe any copyright, database rights, trademarks or other intellectual property.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, MC enforces a clear desk and screen policy:

- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be handed to LM / office for disposal after use.

Working Off-site

It is not accepted that MC mobile devices will be taken off-site.

Software

Employees must use only software that is authorised by Hurst or MC on Hurst's computers.
Authorised software must be used in accordance with the software supplier's licensing agreements.
Employees must not store personal files such as music, video, photographs or games on MC IT equipment.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates.
Employees must not remove or disable anti-virus software.

Skype / Zoom / WhatsApp etc. Communication / Telephone / Voice / Video Equipment and Software - Conditions of Use

Use of MC voice equipment is intended for business use.
Employees must not use MC's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.
All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Actions upon Termination of Contract

All MC equipment and data, for example laptops and mobile devices including telephones, smartphones, rives, USB memory devices and CDs/DVDs, must be returned to MC at termination of contract.

MC DATA PROTECTION

All MC data or intellectual property developed or gained during the period of employment remains the property of MC and must not be retained beyond termination or reused for any other purpose without permission.

Monitoring and Filtering

All data that is created and stored on MC computers is the property of MC and there is no official provision for individual data privacy.
IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.
MC has the right under certain conditions to monitor activity on its systems, including internet use, in order to ensure systems security and effective operation, and to protect against misuse.
Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2 and the Telecommunications Lawful Business Practice Interception of Communications Regulations 2.
It is your responsibility to report suspected breaches of security policy without delay to your LM or Directors.
All breaches of information security policies will be investigated.
Where investigations reveal misconduct, disciplinary action may follow in line with MC disciplinary procedures.