HART LEARNING GROUP

DATA PROTECTION AND MANAGEMENT POLICY

GOVERNANCE AND CONTROL

Date approved by Group CEO	
Scheduled review date	October 2020
Accountable member of Group SMT	Robert Dale
Responsible member of staff	Dave Hitchen
Document author	Robert Dale

AUDIENCE

Applicable to students?	Yes
Accessible to students?	Yes
Accessible to public?	Yes

PURPOSE

The policy helps us ensure that:

- The Group's commitment to protecting personal data is reinforced.
- Staff understand the rules in governing their use of personal data to which they have access in the course of their work ensuring importance of obtaining consent.
- Data is managed and processed effectively and in accordance with legislation.
- Requests for information are dealt with efficiently and in accordance with legislation.

SCOPE

This policy prescribes our approach to data protection and management within NHC, HL&D, Hart Schools Trust and Group Corporate Services.

DEFINITIONS

- **Data Subject**: The individual whose data the Group is collecting.
- **The Group**: refers to the Hart Learning Group (HLG) and for the purposes of this policy, includes NHC, HL&D and subsidiary companies employing staff for HLG and the Hart Schools Trust.
- **Staff**: for the purposes of this document, the term staff is used to refer to employees, volunteers, agency workers and contractors.

- **Personal data**: information relating to identifiable individuals, such as students, job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data includes (this is an illustrative not a comprehensive list) name, address, other contact details, gender, date of birth, images (including CCTV footage), bank account details, information about previous study or employment and so on. It also includes the Special Category and Sensitive data shown below.

- **Special Category data**: personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), genetic, biometric (where used for ID purposes), physical or mental health or condition, sex life or sexual orientation.

- **Sensitive personal data**: a broader term encompassing Special Category data, but also including personal data about criminal offences, or related proceedings.

RESPONSIBILITIES

The Corporation Board

The Corporation Board, as the Group's governing body, is ultimately responsible for ensuring that personal data is processed fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless there is a clear legal basis for doing so.

There are a number of legal bases for processing personal data likely to be relevant to the Group including the fulfilment of the Group's statutory powers to provide education and training, the fulfilment of a contract, meeting statutory reporting requirements, for the protection of a data subject's vital interests (including health, safety and welfare) and where the individual whose details we are processing has consented to this happening.

It is important that we understand and are clear about why we process personal data.

The Data Protection Officer

The Data Protection Officer (DPO) is responsible for:

- Keeping the Group updated about data protection responsibilities, risks and issues.

- Reviewing all data protection procedures and policies on a regular basis.

- Arranging data protection training and advice for all staff and students.

- Dealing with queries on data protection from staff, students and other stakeholders.

- Responding to individuals such as students and employees who wish to know which data is being held on them by the Group.

- Checking and approving with third parties that handle the Group's data any contracts or agreement regarding data processing.

- Conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

- Co-ordinating with the Director of Communications to ensure all marketing initiatives adhere to data protection laws and this policy.

The Head of Service Delivery

The Head of Service Delivery is responsible for:

- Ensuring that all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

Staff

All staff are responsible for:

- Ensuring that their own personal data held by the Group is accurate and updated as required. For example, if your personal circumstances change, please ensure your records are updated by using the self-service section on Sharepoint.
- Ensuring that any data that they process is kept secure.
- Reporting actual or potential data protection compliance failures.
- Ensuring that they do not use student's personal data for marketing purposes without their prior written consent. This extends to images or personal details in brochures, leaflets, web sites, grades on notice boards, etc.
- Meeting the requirements of this policy.

Students

All students are responsible for:

- Ensuring that their own personal data held by the Group is accurate and updated as required. For example, if your personal circumstances change, please ensure your records are updated by informing Student Services.
- Meeting the requirements of this policy.

DATA PROCESSING

In relation to any processing that involves personal data we will:-

- Review the purpose of the specific processing activity and select the most appropriate basis for that processing i.e:
  - that the processing is necessary for a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
  - that the processing is required to enable compliance with a legal obligation to which the College is subject.

- that the processing is necessary for the protection of the interests of the data subject.
- that the processing is necessary for a specific task carried out in the public interest of official authority by the College.
- that we have the explicit consent of the data subject.

- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices.
- Document our decision as to which lawful basis applies to show our compliance with the GDPR.

Special Category data

- In most cases where special category data is processed, the data subject's *explicit* consent to do this will be required unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work).
- Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

- The Group will ensure that any personal data that is to be processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.
- The Group will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
- Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is accurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

STORING DATA SECURELY

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed. This can be done either in person or by placing the paper records in the confidential waste bins.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on memory sticks etc. must be locked away securely when they are not being used.
- The DPO must approve any cloud service used to store data
- Servers containing personal data must be kept in a secure location, away from general office space.

- Data should be regularly backed up in line with the Group's backup procedures.
- Data should only be copied to a personal device only if there is a legitimate need to do so and only if there is no alternative. Once it is no longer necessary you must completely remove the data from your device including any email attachments containing data.
- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

DATA RETENTION

- Personal data should not be retained for longer than is necessary.
- What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. A copy of these can be found in the Retention and Disposal Policy held on SharePoint.

TRANSFERRING DATA INTERNATIONALLY

- There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

DATA SUBJECT REQUESTS

- In line with legislation, individuals are entitled, subject to certain exceptions, to request access to information held about them.
- Subject access requests should be referred to the DPO. However, teams, departments and individual staff who hold personal data will have to conduct searches of their records themselves in order to respond to subject access requests, so it is in everyone's interests that data is stored in a structured and searchable way.
- Upon request, a data subject should have the right to receive a copy of their data in a structured format.
- These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.
- A data subject may also request that their data is transferred directly to another system.
- A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

INFORMATION REQUESTS

- The Group strives to be as open as possible and is pleased to share information about its activities.
- In line with the Freedom of Information Act, the Group will make available information that is requested by students, staff or members of the public.

- Any requests for information other than personal information kept on students and staff will be dealt with in accordance with the Freedom of Information Act.
- Staff and students can be assured that any personal information will continue to be dealt with in accordance with the data protection principles.

CRIMINAL RECORD CHECKS

- All criminal record checks must be justified by law.
- Some Criminal Record checks may be carried out without consent in some cases e.g. Enhanced DBS checks.

DATA AUDIT AND REGISTER

- The Group will ensure regular data audits take place in order to manage and mitigate risks.
- A data register will be maintained by the MIS Team that contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

REPORTING BREACHES

- Staff reporting breaches allows us to:
  - Investigate the failure and take remedial steps if necessary.
  - Maintain a register of compliance failures.
  - Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures.

CONSEQUENCES OF FAILING TO COMPLY

- The Group takes compliance with this policy very seriously.
- The importance of this policy means that failure to comply with any requirement may lead to disciplinary action and may result in dismissal.

TRAINING AND SUPPORT

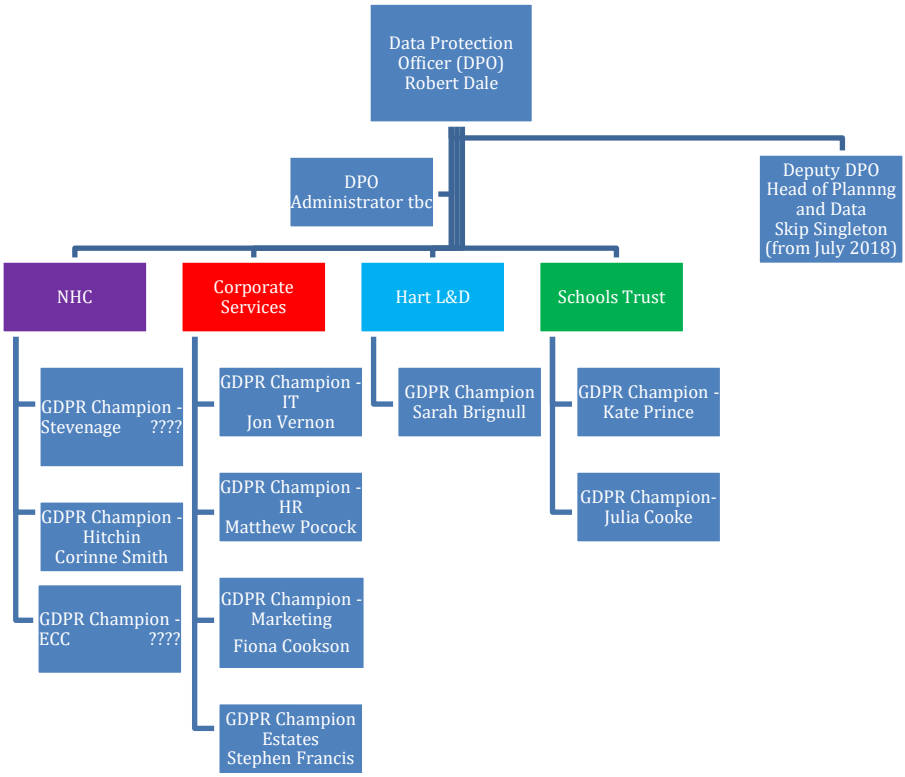
- All staff and students will receive training on this policy.
- Staff can access all information on this policy and a list of useful resources on the GDPR SharePoint page.
- If staff or students have any queries they should direct them to their GDPR Champion in the first instance. (See Appendix A)

LINKED POLICIES / PROCESSES

- IT Management Policy
- IT User's Policy
- Clean Desk Policy
- Business Continuity Policy
- Retention and Disposal Policy
- Bring your own device Policy

APPENDIX A

HART LEARNING GROUP DATA PROTECTION AND MANAGEMENT STRUCTURE



HOW TO HANDLE A SUBJECT ACCESS REQUEST

WHAT IS A SUBJECT ACCESS REQUEST AND HOW CAN ONE BE MADE?

- Any person can request the disclosure of their personal data held by the Hart Learning Group. There is no particular format for doing so – da data subject can simply write or email to ask us to provide all of the information about them that we may hold.
- In principle, a data subject is entitled to receive all of their personal data from us – including data held on paper, in electronic form in any of our systems, contained in emails, CCTV footage, or other media.
- No fee is payable (as was the case under the Data Protection Act 1998), and we have a deadline of one calendar month to respond.

WHAT SHOULD I DO IF I RECEIVE A SUBJECT ACCESS REQUEST?

- If you are asked for disclosure of personal data, please take the following steps immediately:
  - Notify the Data Protection Officer (DPO) (Robert Dale) by email (rdale@nhc.ac.uk) and/or telephone (01462 443066), forwarding any correspondence you have received.
  - Acknowledge the request and advise the requester that, if we hold the information requested and can release it, we will respond within the statutory timescale.

WHAT WILL THE DATA PROTECTION OFFICER DO WHEN A SUJECT ACCESS REQUEST IS RECEIVED?

- Once a request has been received, the DPO will:
  - Satisfy himself as far as possible that the request has come from the person whose personal data we hold (for example, by checking the email, telephone number or postal address used against our records; comparing any signature on the request with any signature held on our records etc).
  - If the request has come from a parent or carer and is in respect of their child, consider whether the young person has given consent or is capable of giving consent for disclosure. The DPO will consider also whether there are circumstances that may make it inappropriate to disclose certain information (such as family separation).
  - Consider whether third parties (such as a Funding Body (the Education and Skills Funding Agency (ESFA) or devolved authorities) must be notified or the request.
  - Ask relevant managers in the parts of the business likely to hold the personal data of the data subject or the information requested by the data subject to

conduct a search of systems and archives (including the Outlook email system and paper records) to locate the personal data requested, and to provide scanned copies in pdf form of any documents and records located.

- Consider what redactions need to be made to the data subject's personal data to avoid the unfair processing of third party personal data or for other reasons permitted by Data Protection legislation and arrange to have such redactions made.

WHAT ELSE CAN DATA SUBJECTS DO?

- Data Subjects can ask to have their personal data corrected, if it is inaccurate; this is known as the 'right to rectification'. Data subjects must provide evidence as to how their data was inaccurate, and it may be necessary to retain both the new and the old data, as long as our records make clear which is the up-to-date information. If we disagree with the data subject's claim of inaccuracy, we may need to record the fact that the accuracy of the data concerned is disputed

- Data Subjects can ask to have their personal data destroyed. This is known as the 'right to erasure' or the 'right to be forgotten'. This right is not absolute; it only applies if (a) we no longer need the personal data; (b) consent previously given by the data subject has been withdrawn; (c) the personal data has been collected illegally; or (d) the data subject has objected to our use of the data and their interest outweigh ours.

- There are likely to be few situations in which these rights arise. However, the same process as applies for acknowledging subject access requests should be followed and the Data Protection Officer will take equivalent actions to address them.

WHAT MUST I DO IF I BECOME AWARE OF A POTENTIAL LOSS OF PERSONAL DATA?

- Personal data must be protected at all times and we are all individually responsible for the security of the data we hold. However, there may be situations in which data is mislaid, disclosed to the wrong person, stolen, or otherwise miscommunicated.

- For example, we may inadvertently send information by email to the wrong person, perhaps because we have used 'reply all' on an email chain, or because the autocomplete function has put the wrong email address into the address box. We may have identified the wrong person on one of our systems, or we may have had information stolen (eg from a laptop bag in which paper records were also being transported) or hacked.

- If you become aware of a potential loss of data you must immediately notify the Data Protection Officer (DPO) (Robert Dale) by email (rdale@nhc.ac.uk) and/or telephone (01462 443066) identifying the circumstances of the loss and the nature of the data affected.

WHAT WILL THE DATA PROTECTION OFFICER DO?

- If a potential data breach is notified the DPO will immediately:

  - Record the notification including an outline of the circumstances and the data affected.

- Undertake an assessment of the circumstances to identify (a) if personal data has been lost; and (b) what potential impact this may have on the data subject.
- Document the assessment and the decision reached about reporting the loss to the Information Commissioner's Office (ICO).
- Consider whether to report the loss to the ICO (all data breaches must be recorded, but not all need be reported).
- Consider whether other parties (eg funding bodies) need to be notified of the loss.

WHAT MUST I DO IF I RECEIVE A REQUEST FROM A THIRD PARTY FOR THE DISCLOSURE OF PERSONAL DATA?

- If you receive a request (eg from the Police or another authority) seeking disclosure of personal data, you must immediately notify the Data Protection Officer (DPO) (Robert Dale) by email (rdale@nhc.ac.uk) and/or telephone (01462 443066) including information about the request and the contact details of the person making it.
- The DPO will consider whether disclosure is appropriate and whether any other party (eg a funding body) needs to be notified.