Data Protection and Information Management Policy

Reviewed by Resources Committee
Approved by Governing Body, December 2018
Next review December 2020
Statutory

1. INTRODUCTION

Hanover collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable us to provide education and other associated functions and to comply with our statutory obligations.

This policy is intended to ensure that the personal information we collect is dealt with correctly and securely and in accordance with the Data Protection Act 2018 and the General Data Protection Regulation 2016. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

2. DATA PROTECTION

Definition of Personal Information

Personal information is defined as data which relates to a living individual who can be identified from that data, or other information held, and provides specific information about them, their families or circumstances. This includes any expression of opinion about an individual and intentions towards an individual, including, but not limited to, their name, address, date of birth, bank details, medical information, address, and contact details (eg email address and computer's IP address). It also applies to data held visually in photographs, video clips (including CCTV footage), or sound recordings, and includes cookies and RFID tags where these leave traces which can be triangulated with other information to create profiles that identify individuals.

In the context of Hanover, this includes:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

The General Data Protection Regulation 2016 and Data Protection Act 2018 also define certain classes of personal information as 'special category data' where additional conditions must be met for that information to be used and disclosed lawfully. Special category data is information that relates to an individual's ethnicity / race, religious or philosophical belief, sexuality, marital status, disability and health, political opinions, trade union membership, or genetic and biometric information.

Data Protection Principles

The General Data Protection Regulation 2016 and Data Protection Act 2018 establish nine enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly, lawfully and transparently;
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in a manner that is incompatible with these purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the General Data Protection Regulation 2016 and Data Protection Act 2018;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.
9. Accountability - the school must demonstrate how it complies with the principles.

Further details are available on the Information Commissioner's website[1].

Hanover is committed to maintaining the above principles at all times. Therefore the school will use its best efforts to ensure that we:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom it was shared;
- Ensure that we hold the minimum personal data necessary to enable us to perform our functions;
- Check the quality of the information we hold to ensure that it is accurate and up to date and that inaccuracies are corrected without unnecessary delay;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests and Education Records Requests; and
- Ensure our staff are aware of and understand our policies and procedures

Under the Data Protection Act 2018 and the General Data Protection Regulation 2016, schools have a duty to issue a Privacy Notice to all pupils/parents and staff, summarising the information held on them, why it is held, and the other parties to

[1] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/principles/

whom it may be passed on. Our Privacy Notices for information held about pupils and staff are available on our website. They are also included at Appendices A and B of our Access to Information Policy.

Registration

Hanover is registered as a Data Controller on the Data Protection Register, held by the Information Commissioner's Office (ICO). The Register details the information we hold and process, and can be accessed on the following website:
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

3. RESPONSIBILITIES

Overall responsibility for ensuring that Hanover meets the statutory requirements of the Data Protection Act 2018 and the General Data Protection Regulation 2016 lies with the Governing Body as the data controller. The Governing Body has delegated day-to-day responsibility to the Head teacher. The Head teacher has nominated Hanover's School Business Manager as the School's Senior Information Asset Owner (SIAO).

As SIAO, the School Business Manager will keep up to date with current legislation and guidance and will:

- Ensure compliance with this policy within the school;
- Take responsibility for the performance of risk assessments and data protection impact assessments in respect of the data we hold; and
- Appoint Information Asset Owners in consultation with the Head teacher.

Hanover will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

The designated Data Protection Officer (DPO) is independent, having no role in handling personal data, and will report directly to the Head. They are responsible for:

- Informing and advising the School and our employees about their obligations to comply with the GDPR;
- Monitoring compliance with the GDPR, including advising on data protection impact assessments and on training for staff, conducting internal audits, and reporting breaches to supervisory authorities, such as the Information Commissioner's Office; and
- Being the School's first point of contact for supervisory authorities.

It is the responsibility of all members of our school community to take care when handling, using or transferring personal data. This should be done in a way that personal / special category data cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Anyone who is involved with the collection, processing and disclosure of personal data or who has access to personal / special category data must know, understand and adhere to this policy. This includes not only school staff and governors, but also relevant contractors / delivery partners working for the school.

All staff and governors will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff and governors
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners.

Governors are required to comply fully with this policy in the event that they have access to personal / special category data, when engaged in their role as a Governor.

4. DATA HANDLING AND SECURITY

General principles

Hanover and our employees will do everything within our power to ensure the safety and security of any material of a personal or sensitive nature that we hold.

All personal data will be fairly obtained in accordance with our Privacy Notices and lawfully processed in accordance with the "Conditions for Processing".

Conditions for Processing

In line with the Data Protection Act 2018 and the General Data Protection Regulation 2016, Hanover will only hold and process personal data if at least one of the following conditions is met:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to the school (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests" - that is, only in cases of life or death.
- The processing is necessary for administering our statutory functions.
- The processing is necessary for the School's legitimate interests, unless there is a good reason to protect the individual's personal data which overrides these legitimate interests.

Additional conditions for processing are required for special category data. Further guidance is available from the Information Commissioner's website.[2]

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

The School will seek consent from the individual to the processing of data. We will seek to ensure that this consent is freely given, specific, informed, and unambiguous, and with a positive opt-in. We will seek to obtain explicit consent either in written format or verbally, such that the consent can be verified. The School is not required to obtain consent for the processing of data:

- When a child is believed to be at risk of significant harm;
- When safeguarding the child's welfare overrides the need to keep the information confidential;
- When instructed to do so by a court;

and when the processing is required:

- In order to perform a statutory function;
- In order to prevent fraud or assist with the prevention, detection or prosecution of a major crime.

Risk Assessments

Information risk assessments will be carried out annually by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising and mitigating the risks.

Data Protection Impact Assessments

The School will carry out a Data Protection Impact Assessment when considering using data in new ways or when implementing new IT – for example, the purchase of a new system that holds personal data, the installation of a new CCTV unit, and the introduction of the monitoring of the IT usage of pupils / staff.

Secure storage of and access to data

Hanover will ensure that it has systems and procedures in place to keep personal / special category data secure and control access to these. Access to protected data will be controlled according to the role of the user.

All users will use strong complex passwords which must be changed regularly as per our E-safety policy. User passwords must never be shared.

Personal / special category data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal / special category data can only be stored on school equipment (this includes computers and portable storage media (where allowed)). Private equipment (i.e. owned by the users) must not be used for the storage of personal / special category data.

When personal / special category data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be encrypted and password protected - many memory sticks / cards and other mobile devices are not encrypted and cannot be password protected;
- the device must offer approved virus and malware checking software, where applicable - memory sticks will not provide this facility and most mobile devices will not offer malware protection; and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Hanover has procedures in place for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

Hanover is aware that data held in remote and cloud based storage systems is still required to be protected in line with the Data Protection Act 2018 and the General Data Protection Regulation 2016, and that, consequently, were it to use such systems, it would need to ensure that it was satisfied with controls put in place by remote / cloud based data service providers to protect the data.

Further guidance on the use of cloud based storage systems is available from:

- the ICO (see appendix for further information and the ICO Guidance: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx; and
- The Department for Education. https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

A list of “do’s” and “don’ts”, setting out good data security practice for individuals, is at Appendix A.

5. RECORDS MANAGEMENT

General principles

Hanover recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

Scope

This policy applies to all records created, received or maintained by staff, governors and other stakeholders of the school in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This will be done in liaison with the London Metropolitan Archives.

Responsibilities

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School, but day-to-day responsibility is delegated to the School Business Manager.

The person responsible for day-to-day records management in the school, the School Business Manager, will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

The School will maintain an Information Asset Register to enable it to demonstrate what information is collected, processed and shared by it.

Individual staff, governors and contractors must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

Hanover's records management guidelines

Hanover has adopted as its records management guidelines the "Information Management Toolkit for Schools" (Version 5, 1 February 2016), issued by the Information and Records Management Society.[3]

6. RECORDS RETENTION

Under the Freedom of Information Act 2000, Hanover is required to maintain a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under the Data Protection Act 2018, the General Data Protection Regulation 2016 and the Freedom of Information Act 2000.

Members of staff, governors and contractors are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to record series regardless of the media in which they are stored.

Hanover's retention schedule is contained in our separate "Information Retention Policy and Schedule".

[3] http://irms.org.uk/page/SchoolsToolkit

7. INFORMATION DISPOSAL

Personal and special category data shall not be kept for longer than is necessary for the School's purposes. The School's Senior Information Officer will ensure that records that are no longer required are reviewed as soon as possible under the criteria set out so that the appropriate records are destroyed.

The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the School for research or litigation purposes.

Whatever decisions are made, they need to be documented as part of the records management policy within the School.

The disposal of personal and special category data, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. Electronic files will be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated. In order to ensure the safe destruction of records, Hanover follows the guidance set out on page 26 of the "Information Management Toolkit for Schools" (Version 5, 1 February 2016), issued by the Information and Records Management Society. [4]

On expiry of their term of office, governors should surrender any confidential information they hold to the School Office for disposal. The same applies to staff and contractors.

In line with the Freedom of Information Act 2000 Hanover maintains a Destruction Log of all data that is disposed of / records which have been destroyed. Details on the log include:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range of destruction
- The name of the authorising officer
- Date action taken

Where records have been identified as being worthy of permanent preservation, arrangements will be made to transfer the records to London Metropolitan Archives. Hanover will contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the Data Protection Act 2018, General Data Protection Regulation 2016, and Freedom of Information Act 2000.

[4] http://irms.org.uk/page/SchoolsToolkit

8. ACCESS TO INFORMATION

Hanover recognises that under Section 7 of the Data Protection Act 2018 and the General Data Protection Regulation 2016, people on whom we hold data have a number of rights in connection with their personal data. They have the right:

- To be informed about how theur data is being used;
- To access their data;
- To rectify incorrect information;
- To have their data erased;
- To restrict how their data is used;
- To object how their data being used at all; and
- To move their data from one organisation to the other

More details on an individual's right to access their data and how to make requests to access the data we hold are given in Hanover's Access to Information Policy. The policy also details circumstances in which other parties have rights of access to the information we hold.

9. DATA BREACHES

Under the General Data Protection Regulation 2016 a data breach is defined as:

> "A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Data breaches can have serious consequences on individuals and/or institutions concerned, can bring the school into disrepute, and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office on the school and individuals involved. Transfer of data is particularly subject to greater risk of loss or theft.

All staff must report any suspected data breach to the School Business Manager, as the School's SIAO, without delay. The SBM will then review the incident and pass details on to the DPO as quickly as possible. The DPO will then pass details of the incident, and of the action the School is taking to address the breach, in cases where the breach results in a **risk** to the rights and freedoms of the individual whose data was affected. The School has to report the data breach within 72 hours (<u>not</u> working hours) or it could face substantial fines.

The School will also inform those individuals whose data was affected where the breach could pose a **high risk** to their rights and freedoms.

The School will also inform governors of any data breach reported to the DPO as soon as is reasonably possible.

10. COMPLAINTS

Complaints relating to information management will be dealt with in accordance with the school's complaints policy. If the outcome is not satisfactory, then complaints can be referred to the Information Commissioner's Office (the statutory regulator).

11. REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the Headteacher, or nominated representative.

The School Business Manager will report annually to the Resources Committee of the Governing Body on the implementation of the policy. The Report will include, but not be limited to, notifications of data requests made, the performance of information risk assessments, the disposal and destruction of data, and breaches of this policy during the year – see Appendix B.

12. CONTACTS

If you have any enquires in relation to this policy, please contact the School Business Manager at admin@hanover.islington.sch.uk who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745.

APPENDIX A – GOOD SECURITY PRACTICE

Updated October 2017 gdpr.lgfl.net

Data Security – Do's and Don'ts for school staff

Passwords – Do

- use a strong password (see the National Cyber Security Centre advice)

Passwords – Don't

- share your passwords with anyone else or write them down
- save passwords in web browsers if offered to do so

Devices – Do

- try to prevent people seeing you enter passwords or view sensitive information
- log-off / lock your device when leaving it unattended

Devices – Don't

- use personal devices to view school-related or pupil data

Sending and sharing – Do

- be aware of who you are allowed to share information with. Check with your school data protection officer if you are not sure, who will check that third parties are GDPR-compliant
- only use encrypted removable media (such as encrypted USB pen drives) if ever taking any personal or sensitive data outside your school (which should be avoided and only done with permission)

Sending and sharing – Don't

- send sensitive information (even if encrypted) on removable media (USB drives, CDs, portable drives), if secure remote access is available.
- send sensitive information by email unless it is encrypted and use the systems that you are told to use

Accessing / saving data – Do

- only attempt to access data you are allowed to and save it on locations where your school knows that data is stored (the school must know where all data is and be able to access it)

Working on-site – Don't

- leave sensitive information unattended; lock it away in lockable drawers or log off or lock your work station
- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site – Do

- only take information offsite when you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- access data remotely instead of taking it off-site using approved secure systems
- make sure you sign out completely from any services you have used
- ensure you save to the appropriate directory to enable regular backups

APPENDIX B – ANNUAL DATA MANAGEMENT REPORT TO GOVERNORS - YEAR:

School's handling of information requests during year

Type of request	Number of:			Comments (optional)
	Requests made	Requests refused	Cases where statutory deadlines missed	
FoI requests				
Environmental information requests				
Subject Access Requests				
Requests to access pupil records/files				

Data breaches during year

Relevant training undertaken during year

Note: School's compliance with website disclosure requirements is monitored separately by governors

Signed:

Date: