NOTTINGHAM HIGH SCHOOL

Data Protection Policy

This Policy applies to the whole school and all staff including those in the EYFS

NOTTINGHAM HIGH SCHOOL

Contents

1. Introduction

The General Data Protection Regulation (GDPR) 2016 is the law intended to strengthen and unify data protection for individuals within the European Union. It also addresses the export of personal data outside the EU. It applies to anyone who handles or has access to people's personal data and therefore applies to all staff at the School.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

This policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

In particular, this policy requires staff to ensure that the Director of Finance and Operations be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed by the School. For example, where we implement new software which requires the School to provide personal data for the purpose of the new service – as we did for the new cashless catering service – or, where we decide to offer a service to our students delivered by a third party which means we provide some personal data – we provide health screening provided by the NHS for our students.

2. Definitions and scope of the Policy

Data Protection Compliance

The School has a legal responsibility to comply with the GDPR. The School, as a corporate body, is named as the Data Controller under the regulation. The School has appointed the Director of Finance and Operations as the Compliance Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Director of Finance and Operations, Headmaster or the Head of IJS.

Personal Data means any information relating to an identified or identifiable natural person. "Identifiable" means one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity. This means that a document might contain Personal Data about someone even if they are not named, (eg, if it was obvious who was being referred to).

Sensitive Personal Data includes information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health or condition, sexual life, actual or alleged

criminal offences and sentences imposed. Sensitive Personal Data will generally be processed only where one of the following conditions applies:

- The Data Subject has/have given explicit consent
- The processing is necessary to protect vital interests
- There is a medical or statutory requirement to process the data

Processing may include creating, obtaining, recording, holding, disclosing, amending, destroying or otherwise using personal data. This means that the School will be caught by the GDPR just by storing Personal Data. The School will process a wide range of Personal Data of pupils, their parents or legal guardians, staff, volunteers and Governors as part of its operation.

The purposes for which personal data may be used by us include:

- Compliance with our legal, regulatory, governance and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring school policies are adhered to (covering email and internet use for example)
- Operational reasons such as admissions, timetable planning, co-curricular support and all aspects of delivery our service to students and their parents
- Investigating complaints
- Checking references
- Monitoring and managing staff access to systems and facilities
- Monitoring staff absences, conduct and discipline.
- Marketing our school

Exemptions from the provisions of the GDPR includes Personal Data processed in connection with the prevention or detection of crime and National Security. Any further information on exemptions should be sought from the Director of Finance and Operations.

The GDPR applies to Personal Data held on computer. This is the case regardless of how the information is held. For example, Personal Data stored in an email, in a spreadsheet, ISAMS or on a smartphone, are all caught by the GDPR. Recorded CCTV images and sound recordings will also contain Personal Data.

The GDPR also applies to most paper records. Best practice is to treat all paper records as being covered and therefore be subject to the GDPR. Virtually any information about someone is likely to be Personal Data. All of the following school related examples are likely to contain Personal Data and are therefore subject to the GDPR:

- Information about a child protection incident
- A record about disciplinary action taken against or an investigation into a member of staff
- Photographs of pupils
- A tape recording of an interview or meeting
- Contact details and other personal information held about pupils, parents and staff and their families
- Contact details of a member of the public who is enquiring about placing their child at the School

- Financial records of a parent
- Application forms and associated interview records
- Records of staff sickness absence or compassionate leave.

The School will regularly audit and update a Data Register to manage and mitigate risks where possible. The register will contain information on what data is held, where it is stored, how it is used, who is responsible for the data, the legal bases for processing and any other regulation or retention timescale that may be relevant. The Data Register will be accessible to the whole School on a read only basis and will be maintained within the Operations Department. Dave – can you check this is the case please.

3. Data Protection Principles

The GDPR is based on six data protection principles, or rules for 'good information handling'. All staff should be aware of these and take personal responsibility for the practical application of this policy. Practical guidance on how this relates to School life are detailed in section 4 below.

1. Data must be processed fairly, lawfully and in a transparent manner in relation to individuals. There are six lawful bases for processing data:
    - Consent
    - Contract
    - Legal Obligation
    - Vital interests
    - Public Task
    - Legitimate interests.
2. Personal data shall be obtained only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose;
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest (including safeguarding), scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Practical Data Protection in School

Legal bases of Processing Personal Data - Personal Data should only be used for specific and legitimate interests. In the case of the School these are:-

- Providing pupils and staff with a safe and secure environment, an education and pastoral care – legitimate interest and contractual
- Providing activities for pupils and parents - this includes school trips and activity clubs – legitimate interest for academic and consent for co-curricular
- Providing academic and examination references for pupils – legitimate interest
- Providing employment references for pupils and staff - legitimate interest
- Administering the recruitment and employment of staff - contract
- Safeguarding and promoting the welfare of children – legal obligation
- Protecting and promoting the interests and objectives of the School - this includes fundraising – legitimate interest
- Fulfilling the School's contractual and other legal obligations. – Contract and legal obligation

School staff must not Process Personal Data for any other purpose without the Director of Finance and Operations permission.

Staff should not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the Director of Finance and Operations permission.

Disclosing Personal Data - Staff will frequently disclose Personal Data for legitimate professional purposes. For example, staff may routinely discuss a pupil's academic progress with parents. This is allowed by the GDPR, but staff will need the permission of the Director of Finance and Operations before they:-

- disclose Personal Data in circumstances which might be considered unusual
- where the Personal Data includes Sensitive Personal Data
- transfer Personal Data outside the European Economic Area (EEA)
- disclose personal data (e.g. grades; positions in exams) relating to any other student or their families when discussing such matters relating to their tutees.

Handling Personal Data in general

- Staff must not use Personal Data for any purpose that is incompatible with the purpose for which it was originally acquired without obtaining the individual's consent. Staff should seek advice from the Director of Finance and Operations in all but the clearest of cases, but if information has been obtained in confidence for one purpose, it must not be used for any other purpose without authorisation from the Data Subject
- The School must process Personal Data in a way that is fair to individuals. Following this policy is likely to mean that the processing is fair in most cases. However, the concept of fairness can be quite difficult to define and staff should inform the Director of Finance and

Operations if they feel that any of the processing of Personal Data appears to be unfair to any individual in any way even if the processing appears to comply with this policy.

- The School must only keep Personal Data for as long as is reasonably necessary but staff should not delete records containing Personal Data without authorisation. Staff should consult the School's Records Management Guidance for guidance on data retention.
- Staff should ensure that Personal Data is complete and kept up-to-date. For example, if a parent notifies a member of staff that their contact details have changed, the member of staff should inform the School's Database Manager so that the School's central record can be updated.
- The School must ensure that it has sufficient Personal Data. For example, a teacher writing a report about a pupil should ensure that he/she has all the pupil's relevant records including learning support information to hand.
- The School must not process Personal Data in a way that is excessive or unnecessary. For example, where 8 pupils out of a class of 20 attend a field trip, the member of staff should only take records (such as information about allergies and parent contact details) of those 8.
- Personal Data held on individual staff personal files must relate only to that individual. For example, payroll instructions must be specific to the individual concerned, or on separate sheets for filing. This is to ensure that Personal Data of staff is not disclosed inadvertently.

Informing the individual - Individuals must be told what data is collected, and what it is used for, unless it is obvious. This is called a privacy notice or fair processing statement. Individuals should also be told which third parties (if any) it will be shared with and anything else which might be relevant.

Staff are not expected to routinely provide pupils, parents and others with a privacy notice as this should have already been provided in the parent contract and copies of the parent and pupil privacy notices can be found on the School's website. Having said this, staff should inform the Director of Finance and Operations if they suspect that the School is using Personal Data in a way which might not be covered by an existing fair processing notice. This may be the case where, for example, staff are aware that the School is collecting medical information about children without telling their parents what that information will be used for.

Sharing Personal Data - The general position is that Personal Data should only be shared on a "need to know" basis. Before sharing Personal Data staff should:

- Make sure they are allowed to share it
- Ensure adequate security (please see section 5 below)
- Make sure that the sharing is covered in the School's privacy notices for pupils and parents.

Sharing Personal Data within the School - This section applies when Personal Data is shared within the School. Personal Data should only be shared within the School on a "need to know" basis although this will not prevent sharing Personal Data where doing so is reasonable and proportionate and is done in accordance with this policy and on the understanding that the Staff Code of Conduct applies to all aspects of confidentiality within school.

Staff should think about whether the person(s) they wish to share the Personal Data with needs access to the information. Good examples of sharing which are *likely to comply* with GDPR include:

- A teacher discussing a child's academic progress with other members of staff (for example, for advice on how best to support the child)
- Informing an exam invigilator that a particular pupil suffers from panic attacks
- Disclosing details of a persons allergy to bee stings to colleagues so that they will know how to respond. Other private health matters must still be kept confidential and advice should be sought from the Operations Manager if in doubt.

Good examples of sharing which are *unlikely to comply* with GDPR include:

- The Head being given access to all records kept by nurses or counselling staff working within the School (seniority does not necessarily mean a right of access)
- Disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or unless it is an emergency).
- Sharing academic data with a pupil that also shows the data relating to other students.

Sharing Personal Data with individuals and organisations outside of the School (for example, with other schools, colleges, social services, the Police, and contractors) is often permissible so long as doing so is fair and lawful under GDPR. Staff should always speak to the Director of Finance and Operations if in doubt, or if staff are asked to share Personal Data in a new way.

Before sharing Personal Data outside of the School, staff should:

- Make sure that they are allowed to share it
- Ensure adequate security (please see section 7 below). What is adequate will depend on the nature of the data. For example, if the School is sending a child protection report to social services on a memory stick then the memory stick must be encrypted
- Make sure that the sharing is covered in the privacy notices for pupils and parents (please see section 7).
- The School should ensure that any emails which contain attachments with Sensitive Personal Data in are encrypted. This includes emails sent to parents.
- Staff should not disclose Personal Data to the Police without permission from the Director of Finance and Operations, Headmaster or the Head of IJS (unless it is an emergency). The Police are required to request Personal Data formally using an appropriately worded form and through a secure email.
- Staff must not disclose Personal Data to contractors without permission from the Director of Finance and Operations, Headmaster or the Head of IJS. This includes, for example, sharing Personal Data with an IT contractor (e.g., where the contractor is to carry out a data cleansing exercise).
- Staff should be aware of the use of deceit to obtain personal data from people or organisations. Staff should seek advice from the Director of Finance and Operations, Headmaster or the Head of IJS where staff are suspicious as to why the information is being requested or if they are unsure of the identity of the requester (e.g. if a request has come from a parent using a different email address).

5. Data Security and staff responsibilities

Information security is the most important aspect of data protection compliance. Most of the fines under the Data Protection Act 1998 related to security breaches such as leaving an unencrypted memory stick in a public place, sending sensitive documents or information to the wrong recipient, leaving a computer screen on and unlocked with personal data accessible, leaving printed information on the teacher's desk, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web. Under GDPR, the scale of fines has increased dramatically which increase risks associated with any security breaches significantly. Staff must do all that they can to ensure that Personal Data is not lost or damaged, or accessed or used without proper authority and must be familiar with and comply with all associated school policies and procedures.

GDPR requires the School to take organisational measures (for example, ensuring that staff are trained on information security), and technical measures (for example, encryption, secure shredding etc) to ensure that Personal Data is kept secure.

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to staff, parents, ON, governors and pupils.

Where a member of staff is permitted to take data offsite it will need to either be encrypted or kept secure at all times. School recognises that staff will need to access personal data from home or remotely for the fulfilment of their duties and responsibilities and staff will be supported to identify suitable technical and organisational solutions to this practical requirement.

Staff must

- Immediately report all security incidents, breaches and weaknesses, to the IT Manager. This includes anything which the member of staff becomes aware of even if they are not directly involved (for example, if a teacher notices that document storage rooms are sometimes left unlocked at weekends) or if documents are left lying around in the staff room – please take particular care when printing to remote printers.
- Be very careful when sending correspondence containing Personal Data (e.g., sending an email, or sending documents by post). Staff should check that they are sending the correct Personal Data to the intended recipient very carefully and ideally should ask an appropriate colleague to check both the data to be sent and the individual recipient for accuracy.
- Extreme care must be used with attaching files to emails.
- Comply with all School procedures relating to the handling of Personal Data and use of IT equipment.
- Not use or leave computers, portable electronic devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons. Staff should take

reasonable steps to ensure that such devices are not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

- Be vigilant of the risks posed by cameras on mobile phones. As such, Sensitive Personal Data should always be carried in sealed envelopes / folders to avoid it being photographed.
- The School uses a range of measures to protect Personal Data stored on computers, including, anti-virus and security software, user passwords, and back-up systems. These should be used in all cases.
- Staff must ensure that all electronic data is stored in a School approved location – internal network or in the School's chosen cloud service. If in doubt, please contact the IT Manager.
- When staff need to access personal data from home or remotely, they should use the remote desktop facility (ie ISAMS and Office 365).
- Not download Personal Data relating to the School to their own computers or send such Data to their own email accounts. For example, they must not send School related emails containing Personal Data to their private email account.
- Not allow unauthorised access to School computers or other computers containing School related Personal Data. For example, staff should not allow pupils or their friends and family access to their work computers or work emails.
- Use bcc (blind carbon copy) where appropriate. ISAMS is a more secure email facility for large scale communications with parents.
- Lock their computers when not in use at all times.
- Keep any passwords secure although passwords are not always effective and are not a substitute for encryption. Passwords should contain at least eight characters, use special symbols, be difficult to guess, and should be changed frequently.
- Encryption should be used, when handling personal, sensitive or confidential data. This includes saving internally on the approved school systems and when transferring data to external entities (please refer to the document How to Encrypt which can be found within the IT Guidance on SharePoint).
- Ensure that personal data held in hard copy/paper form are kept under lock and key in a secure location.
- Take extra precautions in relation to any Sensitive Personal Data and any Personal Data which is particularly confidential, both of which should be stored in a storage room or in a strong cabinet (again under lock and key).
- Ensure that documents containing Personal Data are never left unattended on desks.
- Comply with the School's Internet and email policy for staff 2020.

Staff must not

- Do anything to compromise the security of any of the School's systems.
- Change any privacy settings or connect any device that has not been provided by the School (such as a memory stick)

- Click any links in documents or emails, unless the member of staff is absolutely sure that source is trusted.
- Store School information in third party cloud service providers such as Apple iCloud, Dropbox or Google Drive.
- Synchronise the School's cloud services with non-School devices.
- Attempt to gain unauthorized access to any part of the School's ICT system.

Some School Personal Data is so sensitive that it should never be taken off site, and / or accessed by staff using their own devices, without specific permission from the Director of Finance and Operations, Headmaster or the Head of IJS or where the School has special arrangements in place for the safe management of school trips. This includes:-

- Information concerning child protection matters
- Information about serious or confidential medical conditions and information about special educational needs
- Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved)
- Financial information (eg, about parents and staff)
- Any other information which falls within the definition of Sensitive Personal Data under GDPR. (see section 2 above)

6. Retention schedule and Disposing of Personal Data

Any record containing Personal Data should be securely destroyed, in accordance with the appropriate retention period as indicated in the Schools Records Management Guidance. The School follows the Information and Records Management Society Retention Guidelines for Schools which is available on Sharepoint or from the EA to the Headmaster or the Operations Manager.

Personal Data must not be kept for longer than is necessary and any paper documents should be shredded or placed in the confidential waste bins provided located in Finance or the Staff Workroom. Cross cut shredders can be located in the Operations Office, Art Department, Examinations Officer Office and with the EA to the Headmaster. CDs, memory sticks and other storage media should be physically destroyed when they are no longer required. When disposing of computer records containing Personal Data it is important to make sure that the record is permanently deleted. It is not sufficient just to move the file into the recycle bin. Specialist software should be used to permanently delete the computer record. Further information is available from the IT Manager.

All paper records should be disposed of securely. For example, if a member of staff is working from home then they should return any paper waste to the School to be securely disposed of.

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Archives.

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

7. Rights of Individuals

Individuals have a number of rights under GDPR.

1. The right to be informed relates to the School's obligation to provide 'fair processing information' typically through a privacy notice. The School's HR Privacy Notice applies to all staff and the student and parent privacy notice is accessible via the website.
2. Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

   This is one of the most commonly exercised rights - to request a copy of the Personal Data the School holds about them. This is called a Subject Access Request. Any staff who receives a Subject Access Request must promptly forward it to the Director of Finance and Operations, Headmaster or the Head of IJS, which should be on the same day. This is important as there is a statutory procedure and timetable which the School must follow. Staff must never respond to a Subject Access Request themselves. Staff should be aware that there is no obligation to refer to any legal bases for the request or to use the phrase "Subject Access Request" when making a request. By way of an example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request.

   Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should a Subject Access Request be made. There is no exemption for "embarrassing" information. For example, an exchange of emails containing gossip about an individual will usually be disclosable. As such, staff must be aware that anything they put in an email is potentially disclosable.

3. GDPR gives individuals the right to have personal data rectified and the School has one month to respond to requests for rectification. Any staff who receives a request for data to be rectified must promptly forward it to the Director of Finance and Operations, Headmaster or the Head of IJS, which should be on the same day.

4. GDPR gives individuals the right to erasure or the right to be forgotten. Any such requests for staff would need to be considered in the wider context of safeguarding but for former students this could be a legitimate request.

5. GDPR gives individuals the right to block or suppress processing of personal data. This is not likely to affect school.

6. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This is not likely to affect school.

7. Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. Specific school example might relate to ONs asking school to stop contacting them or for parents asking school to stop emailing them with school promotional messages.

8. The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. This is not likely to affect school.

8. Further information and guidance

If staff have any questions about this policy or about data protection they should speak to the Director of Finance and Operations, the Operations Manager or the IT Manager. Similarly, all staff have an obligation to assist the School and colleagues to comply with GDPR. Staff must report any concerns, or any evidence of noncompliance, to the Director of Finance and Operations.

We have registered our use of Personal Data with the Information Commissioner's Office and further details of the Personal Data we hold, and how it is used, can be found in our register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z5488755. This website also contains further information about data protection.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.