NORTHGATE
High School

Data Protection Policy

Introduction

The Data Protection Act 2018 concerns personal privacy and regulates how information about living individuals may be collected, used, retained and disclosed. All processing of personal data must be notified to the Information Commissioner.

The Act applies to all personal data, whether it is in manual or electronic format. Individuals are entitled to see all information kept about them. Members of staff should be open with individuals about any information held about them. Staff should also be careful about passing any personal information on to third parties.

This policy gives a brief and simple outline of the responsibilities of staff and students under the Data Protection Act 2018.

Data Protection principles

Staff and students must comply with the eight principles governing the legal processing of personal data.

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose(s).
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
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.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area (without the individual's express consent) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Achieving compliance with the Data Protection principles

Principle 1

No personal data should be created or held unless the individual has given his/her consent.

Where sensitive data is concerned specific consent must be obtained - the individual must be informed that this type of personal data is being held, told the reason for it and must then agree.

Photographs are classified as sensitive data because they may reveal information about the subject's race and ethnicity. Permission should always be obtained to keep or use a photograph of an individual.

Principle 2

Do not use data obtained for one purpose for a different purpose. For example, a departmental list of members of staff or students should not be used for commercial mail shots.

Principle 3

Do not collect information about individuals which is not absolutely necessary. Do not ask questions seeking data without ensuring that the questions are strictly relevant. If excessive or superfluous personal data is acquired it should be deleted or destroyed immediately.

Principle 4

If data is retained it must be reviewed and if necessary amended or updated. No data should be kept unless it is reasonable to assume that it is accurate.

Principle 5

Regular and systematic reviews of files (both manual and electronic) containing personal data should take place to ensure that information is not retained for longer than is necessary.

Principle 6

The rights of individuals in respect of their data should always be considered. Consent should be obtained if personal data is to be generated or retained for any purpose. Data subjects are legally entitled to know what information is being held about them.

It is also important that no personal data is disclosed to anyone, either inside or outside the school, unless strictly necessary or unless the consent of the data subject has been obtained.

Principle 7

Staff must ensure that any personal data is kept in a secure place; in lockable filing cabinets or in rooms which can be locked when unoccupied. They must also seek to prevent unauthorised access to any computers in which personal data is stored.

Principle 8

No personal data should be transferred, even for a legitimate purpose, outside of the European Economic Area (EEA) except with the specific consent of the data subject. This is particularly important when considering the global publication of personal information via the World Wide Web.

Staff should be aware that publishing personal information on the school's website effectively means that the information is published world-wide and outside the EEA. It, therefore, cannot be protected by the DPA or the European Directive on Personal Privacy. Great care should be taken before publishing any personal information (or any information from which individuals could be identified) in this manner and the approval of both the school's web manager and Data Protection Officer should be obtained before publication.

Rights of the individual

Under the Data Protection Act 2018 individuals have the right to inspect all personal information held about themselves. This includes the contents of student files, staff files, unit enrolment forms, and lists of members of staff who, for example, are on leave.

Data subjects might include staff, students, alumni, job applicants, consultants, former employees, staff of other institutions, governors and members of the public.

Responsibility and Accountability of Designated Personnel

The Chief Information Officer is the Head Teacher and is:

- Responsible for ensuring that the school manages its information and records properly and is compliant with all the relevant legislation.
- Responsible for ensuring the Governing Body is briefed on all relevant information issues and obtaining, where necessary, the appropriate approval for any actions required.
- Accountable for demonstrating compliance with DPA and good practice.
- Is responsible for ensuring that the necessary policies and procedures are developed, implemented and reviewed regularly.

The Data Protection Officer is:

- the responsible officer for data protection at the school.
- accountable to the Information Commissioner for ensuring that the school is fully compliant with the DPA.

Has overall responsibility for:

- Advising on personal information security and risk management.
- Compliance with this policy.
- Approval of procedures where personal information is processed such as:
  - the management and communication of privacy notices;
  - handling of requests from individuals;
  - the collection and handling of personal information;
  - complaints handling;
  - management of personal information security incidents; and
  - outsourcing and off-shoring of personal information processing.
- Provision of expert advice and guidance on DPA matters.
- Interpretation and application of exemptions applicable to the processing of personal information.
- Provision of advice in relation to data sharing projects.
- Ensuring the school has access to legislative updates and appropriate guidance related to the DPA.
- Responsible for providing strategic guidance to the school on managing information effectively and lawfully.
- Completing, submitting and managing notifications to the ICO.
- Implementing, as appropriate, any data protection practices outlined in any mandatory or advisory sectoral codes which apply to the school.

Staff

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and personal information is not disclosed either orally, in writing, electronically or otherwise to any unauthorised person.

All members of staff have an individual responsibility to ensure that they comply fully with the DPA.

It is a disciplinary offence, to knowingly, recklessly or carelessly obtain or disclose personal data. Significant breaches of this

policy could result in the prosecution of the school and / or the individual.

Staff should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under the school's disciplinary procedure.

Notification to the Information Commissioners' Office

The school's Notification will be reviewed annually and kept up-to-date by the Data Protection Officer.

It is an offence under the DPA if the Notification is not kept up-to-date. It is also an offence to use personal data in a manner which has not been notified.

A copy of the school's current Notification can be viewed at the Information Commissioner's Web site: www.ico.gov.uk

It is the responsibility of all staff to advise the Data Protection Officer of any changes to the uses of personal data as soon as they occur so that the Notification can be updated.

Data Processing

Personal Data Held – The school will maintain an inventory of all the categories of personal information that it holds and the reasons for holding that data. Such inventories will be reviewed and updated at least annually and any changes communicated to the Data Protection Officer as soon as they are made so that the school's Notification may be kept up-to-date.

Security of Personal Data – The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. Personal information should be:

- if hard copy:
  - not left lying around;
  - kept in a locked filing cabinet or in a locked drawer;
  - disposed of as confidential waste.

- if electronic:
  - be held on a system that has a designated system manager or administrator who has overall responsible for controlling access to that system;
  - be password protected or kept only on portable media which is itself secure in accordance with the school's Password Management and ICT Acceptable Use Protocols;
  - be deleted in accordance with corporate retention periods and evidence of such deletion recorded to provide for necessary audit trails.

Any incidents where personal data has been lost or disclosed to unauthorised recipients should be immediately reported to the Data Protection Officer who will advise what action should be taken to mitigate the damage and determine whether the incident needs to be reported to the Information Commissioner's Office (ICO).

All external data processing carried out on behalf of the school shall comply with this policy. All contracts with third-party providers, where the processing of personal data is required, shall include a requirement for the contractor to comply with the requirements of the Data Protection Act 2018. Where contractors are managing personal data on behalf of the school, there shall be a requirement to monitor data security as part of the on-going contract management activity. Any data breach must be reported to the school's Data Protection Officer immediately, who will advise on the appropriate action to be taken in mitigation.

Sensitive and High Risk Personal Data – Sensitive personal data is defined in the DPA as information concerning an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life or sexual orientation
- criminal convictions or alleged offences

Extra care must be taken when processing sensitive personal data as additional requirements under the DPA must be met to ensure that the processing is legitimate and safe. The advice of the Data Protection Officer should be sought before any new processing of sensitive personal data commences.

There is also some personal information which is regarded as high risk and therefore a risk assessment should be carried out and additional security precautions should be implemented before processing such information. The Data Protection Officer can advise on suitable security measures. High risk personal information includes, but is not limited to:

- personal bank account and other financial information;
- national identifiers, such as national insurance numbers;

- personal information relating to vulnerable adults and children;
- detailed profiles of individuals;
- sensitive negotiations which could adversely affect individuals;
- large numbers of records containing personal information.

Medical records are classed as sensitive personal data under the DPA and, therefore, additional care should be taken when processing this information. In particular, before disclosing the medical records of anyone as part of a Subject Access Request, the advice of the relevant medical practitioner and the school's Data Protection Officer must be sought as to whether the information should be released or not.

Publication of Personal Data – Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasion, it may be appropriate to publish personal information with the individual's consent. However, in such cases staff must ensure that the consent is fully informed and freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

Staff Records and the Monitoring of Staff – The school will comply with the ICO's employment practices code in relation to the processing of staff personal information. This Code exemplifies good practice and strikes a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. In particular, staff monitoring should only be carried out in accordance with this code of practice.

Data generated by CCTV monitoring must only used in accordance with the ICO's code of practice on CCTV section 9. The use of conventional cameras (not CCTV) by the news media or for artistic purposes such as for film making are not covered by this code as they are subject to special treatment in the DPA. However, this code does apply to the passing on of CCTV images to the media.

Individuals must be informed at the beginning of any call if the telephone call is being recorded in any format. They must be advised what information is being recorded, the reasons for recording the information, whether the information will be shared with anyone else and, if so, whom it will be shared with and for how long the information will be retained.

Retention and Disposal of Data – It is the responsibility of the school to ensure that the personal information that they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected.

When the data is no longer required it must be disposed of safely, in accordance with school records retention guidelines.

Access to Data and Disclosure

Data Subject's Rights – The school will ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information;
- the right to prevent processing in certain circumstances; and
- the right to correct, rectify, block or erase information which is regarded as wrong information.

The school will issue Privacy Notices when personal data is to be processed and adhere to the ICO's code of practice on privacy notices.

Data Subject's Access – If individuals do require access their personal data, unless special arrangements already exist to allow them access to the data, they should be encouraged to complete a subject access request form and submit it to the Data Protection Officer so that the request can be logged, managed and tracked. Even if a form is not completed, the Data Protection Officer should be informed of the request so that it can be processed. It is particularly important that all requests for personal information are passed to the Data Protection Officer unless they fall into one of the special arrangement categories as there are legal requirements that must be met when dealing with these requests. In particular, there are a few exemptions to this right so any concerns about releasing any information should be discussed with the Data Protection Officer prior to release of the information.

If in doubt, it is better not to release the information, as it can always be released at a later date with little harm whereas if released in error it cannot easily be recovered.

Subject Consent – On occasion individuals give consent for the processing of their personal information. Staff must ensure that any consent given for the processing of personal information is fully informed and freely given and that individuals are aware that they may withdraw consent at any time and what the consequences would be if they withdrew their consent.

It is advisable not to rely on consent for the processing of personal data if there is another legitimate criterion for processing which could be applied. Before relying on consent, the school must consider the impact if individuals should refuse or withdraw consent.

If it is deemed that the consent of individuals is necessary, staff should be aware that, in the case of sensitive personal data, individuals have to give explicit consent to the processing. It is therefore good practice to obtain written consent in such cases.

External Disclosure Requests – Requests from external organisations or third parties for personal information about individuals should be passed to the Data Protection Officer for processing unless there is an up-to-date information-sharing/data exchange agreement in place with that organisation or third party. Under no circumstances should any personal information about any individual be passed outside the school without the authority of the Data Protection Officer.

Requesters should be encouraged to complete a Request for Personal Information form and send it to the Data Protection Officer.

Sharing Information Within Northgate High School – Before sharing personal information internally it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the school's disciplinary procedure (and, in exceptional circumstances, in criminal charges). If there is any doubt individuals should seek the advice of their line manager or the Data Protection Officer.

Sharing Information Externally – There are a number of instances where information is routinely shared with partners or outside organisations. An information-sharing/data exchange agreement should be drawn up to cover these instances. The agreement can either cover individual cases of information sharing or cover information sharing with a particular organisation or partner.

Each agreement, as a minimum, must clearly state the information that will be shared, the purposes for sharing, the basis on which sharing is carried out and the responsibilities for handling and maintaining the personal data. Advice on drawing up information sharing and data exchange agreements can be obtained from the Data Protection Officer.

Supporting Material

Data Retention Guidelines: LJW

E-mail Acceptable Use Policy: RJG

Acceptable Use of ICT Policy: RJG

Password Management Protocol: S Novak

Freedom of Information and Records Management Policy: SEB

CCTV compliance checklist: LJW

Information Sharing Protocols / Third Party Agreements: SEB

Declaration of inclusivity

This policy has been drawn up within the framework laid down by our Equality and Diversity Policy and has been evaluated and found to have no adverse impact on students, staff, parents and carers from the different groups that make up our school.

Reviewed July 2022