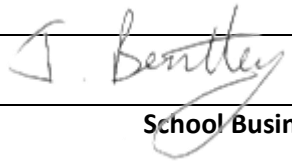
**B1**

# NORTHFIELD SCHOOL

# DATA PROTECTION POLICY

| | |
|---|---|
| **Date adopted** | **June 17** |
| **Signed by Chair of Finance and Resources** |  |
| **Member of staff responsible for monitoring** | **School Business Manager** |
| **Review frequency** | **Biennial** |

| Date | Changes made | Agreed by | Authorised for use by | Date of review |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Location:

# Personal Data Handling Policy

## Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

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

Data breaches can have serious effects 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 - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

*This policy is based on a model template policy created by the South West Grid for Learning (SWGfL). SWGfL have kindly given permission for Northfield School to edit, re-use and publish our document which is closely based on the template they provided.*

### *Guidance*

The DPA (Data Protection Act) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines “Personal Data” as data which relate to a living individual who can be identified (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines “Sensitive Personal Data” as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- their political opinions

- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- their physical or mental health or condition
- their sexual life
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

Guidance for organisations processing personal data is available on the Information Commissioner's Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

## Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

## Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including 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, 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.
- Responsibilities
- The school's Senior Information Risk Officer (SIRO) and Data Protection Officer is the School Business Manager. This person will keep up to date with current legislation and guidance and will:
    - determine and take responsibility for the school's information risk policy and risk assessment
    - appoint the Information Asset Owners (IAOs)

The schools Information Asset Owners (IAOs) are:

- The Senior Leadership Team
- Receptionist
- SENCO
- SEN Administrator

The IAOs will, for the various types of data being held (e.g. student information / staff information / assessment data etc.), 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.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

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

## Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

## Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through schools' website within the policy section. Parents / carers of young people who are new to the school will be provided with the privacy notice through the welcome pack. (Appendix 1)

## Training & awareness

All staff 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
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

## Risk Assessments

Information risk assessments will be carried out 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 the risks.

Risk assessments are an ongoing process and result in the completion of an Information Risk Actions Form (example below):

| *Risk ID* | *Information Asset affected* | *Information Asset Owner* | *Protective Marking (Impact Level)* | *Likelihood* | *Overall risk level (low, medium, high)* | *Action(s) to minimise risk* |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

| *Government Protective Marking Scheme label* | *Impact Level (IL)* | *Applies to schools?* |
|---|---|---|
| **Not Protectively Marked** | 0 | Will apply in schools |
| **Protect** | 1 or 2 | |
| **Restricted** | 3 | |
| **Confidential** | 4 | Will not apply in schools |
| **Highly Confidential** | 5 | |
| **Top Secret** | 6 | |

Most student or staff personal data that is used within Northfield School will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings are shown in the footer e.g.. "Securely delete or shred this information when you have finished using it".

## Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly (at least annually). User passwords must never be shared.

Personal 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 data can only be stored on school equipment (meaning only the schools' networked computers and laptops). Private equipment, portable (i.e. owned by the users) storage media (e.g. USB drives) must not be used for the storage of personal data.

**The school does not allow storage of personal data on removable devices.**

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject.

Requests must be made in writing for the attention of the Senior Information Risk Officer / The School Business Manager. Please note that a charge may be applied for photocopying of resources and the cost of administration (where applicable). There is no charge to read information in-school.

Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

## Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises;
- Users must take particular care that computers which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they must use the school's secure remote access to the management information system and/or our learning platform - ARBOR;
- If secure remote access is not possible, users must NOT remove or copy personal or sensitive data from the organisation or authorised premises to storage media, portable or mobile device;
- The only approved method of secure data transfer is via the encrypted EGRESS email and file-sharing system.

## Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log is kept of all data that is disposed of. The log includes the document ID, classification, date of destruction, method and authorisation.

## Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

## Use of technologies and Protective Marking

Where appropriate, the school will use the following markings:

| | ***The information*** | ***The technology*** | ***Notes on Protect Markings (Impact Level)*** |
|---|---|---|---|
| **School life and events** | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of students work, lunchtime menus, extended services, parent consultation events | School website, emailed newsletters, text messages, social media | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| **Learning and achievement** | Individual student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | ARBORs' secure parental access, communication by email, letter/reports home. | Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make the student record |

| | | | |
|---|---|---|---|
| | | | available in this way. |
| **Messages and alerts** | Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging, ARBORs' secure parental access | Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, the school will not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

## Appendix 1:

# Privacy Notice

## How We Use Information About Students

This notice is provided to all new students, parents and carers and is published on the school's website within the policy section. This notice provides information about the use of students' personal data.

Northfield School uses personal data about its students and is a 'data controller' in respect of this for the purposes of the Data Protection Act 1998. A 'data controller' is an organisation that is responsible for the use made of someone's personal information.

It uses this data to:

- support its students' teaching and learning
- monitor and report on their progress
- provide appropriate pastoral care
- support a young person in their transition to a post 16 provider of education or training
- assess how well the school as a whole is doing.

This data includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

This data may only be used or passed on for specific purposes allowed by law to organisations like:

| | |
|---|---|
| Local Authorities | Department for Education (DfE) |
| Ofsted | Education Funding Agency (EFA) |
| Department of Health (DH) | Skills Funding Agency (SFA) |

All these are data controllers in respect of the data they receive and are subject to the same legal constraints by law in how they deal with the data.

We will also share data with the school's contracted Information Advice & Guidance (IAG) Provider to enable them to support students to progress.

**How Oxfordshire County Council uses this data**

The Local Authority uses information about children for whom it provides services, to enable it to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the child may have.

The Local Authority will share young people's information with post 16 learning providers (e.g. colleges) when it allows the young person to fulfil their statutory duty to participate in learning.

Parents, or the students themselves if aged 16 or over, can ask that no information beyond name and address (for students and parents) be passed on to Post 16 providers. If as a parent, or as a student aged 16 or over, you wish to **opt-out** and do not want Post 16 providers to receive from the school information beyond name and address, then please contact our School Business Manager, who is the school's Senior Information Risk Officer.

Oxfordshire County Council will share information about young people's post 16 learning providers with the school and the school's contracted IAG Provider. They share details of what offers of learning young people have received from other learning providers to make sure everyone has some learning in place for Year 12.

The LA also share information about what young people do after compulsory education for two years after finishing year 11, and until age 24 if the young person has a Learning Difficulty Assessment (LDA) or Education and Health Care (ECH) Plan in place before they leave education.

If you require further information about how the Local Authority (LA) stores and uses your information, then please go www.oxfordshire.gov.uk/cms/public-site/access-data-and-information

If you are unable to access this websites we can send you a copy of this information. Please contact them as follows:

- Oxfordshire County Council
  Subject Access Requests (SAR)
  FIS
  PO Box 876
  Oxford
  OX1 9PB
  Website: www.oxfordshire.gov.uk

  Telephone: 08452 26 26 36

**Further information or queries**

If you have any queries or are concerned in relation to data sharing, you can contact the Council's Information Governance Manager by email or telephone:

Email: information.management@oxfordshire.gov.uk

Telephone: 01865 323593