NP17.1 Data Protection Policy

This policy applies to the whole school including EYFS at Newton Prep

Executive Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

The School monitors its data protection obligations in relation to national data strategy and new technologies the school uses. The school is also cognisant that data that can be sensitive in nature, must be used appropriately in a classroom environment.

Contents

Background

Data protection is an important legal compliance issue for Newton Prep. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers, contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as "data controller", is liable for the actions of its staff, directors and School Council in how they handle data. It is therefore an area where all have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

This Policy will inevitably have some overlap or interaction with our other policies concerning how staff handle data, notably our E-Safety Policy (including Acceptable Use Agreements), Use of Images policy, Retention of Records guidelines, CCTV policy and our Safeguarding and Child Protection Policy (including record keeping and information sharing).

Since Brexit, the General Data Protection Regulation (**GDPR**) is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the Data Protection Act 2018 (DPA 2018). Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The DPA 2018 includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely, and regarding the right of access to personal data.

Keeping Children Safe in Education 2024 (KCSIE) paragraph 54 provides links to the seven golden rules for sharing information and considerations with regard to the DPA 2018 and UK General Data Protection Regulation (UK GDPR). Paragraph 119 of KCSIE specifically confirms that "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law. The School is monitoring its data protection obligations in light of notices issued in relation to other education providers.

Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data and who is legally responsible for how it is used. The School is the data controller of pupils' personal information. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller - for example, visiting music teachers, peripatetic activity instructors, speech therapists
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- **Personal information (or 'personal data')** - any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences. Safeguarding of children and individuals at risk often involves processing special category personal data

Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or directors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter. This policy operates in conjunction with data protection training provided to all staff during INSET, with updates throughout the academic year. Practical matters for staff are covered in the staff handbooks.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

Persons responsible for data protection

The School has appointed the Deputy Head Teaching & Learning, the Head of Digital Learning, the Bursar, the Data Manager and the Compliance Officer as Data Protection Leads who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of UK 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 School's Bursar and a Data Protection Lead.

The Principles

UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Lawful grounds for data processing

Under UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the relatively high bar of what constitutes consent has been tightened under UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller / School. It can be challenged by data subjects and also means the Controller / School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notices, as UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on school business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form that they would be prepared to stand by it should the person about whom it was recorded ask to see it.

Data handling and training

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the School's policies, notably IT - Acceptable Use Agreements, Use of Images policy, Retention of Records guidelines, and our Safeguarding and Child Protection Policy (including record keeping and information sharing).

Staff training outlines matters such as:

- how to adopt to ensure security and confidentiality when sharing personal data internally by email, how to label sensitive emails in the subject line and the use of links and not attachments
- that it is only appropriate to open emails which contain personal data in the classroom environment and the use of systems such as 3Sys, CPOMS and behaviour logs which may contain sensitive or special category data, when children aren't present in the classroom/ teaching and learning space or in the vicinity of the classroom/ teaching and learning space
- encouraging all staff to ask for refresher training when they feel they need it, especially after technical updates to their software (including apps) or hardware, in the use of whiteboards

etc or if they are processing personal data in a new way or adding special category data (e.g SEN information to an app)
- when and how to fill in or update a data protection impact assessment (DPIA) (with templates)
- self-reflective shared responsibility: where can we individually and collectively improve?
- the most common user errors and how to avoid them
- National Cyber Security Centre guidance on the use of passwords and multi factor authentication
- reminders to check the settings on all software used, especially data sharing settings and syncing/linking settings
- a reminder not to enter any personal data into generative AI in accordance with government guidance, and warnings around apps with “virtual friends”
- how to report a breach in accordance with this policy

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in UK GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the Information Commissioner’s Office (ICO) within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. **If staff become aware of a personal data breach they must notify the Bursar immediately (ext 1204, bursar@newtonprep.co.uk).** If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision. Mitigating action can lessen the effects of a personal data breach and the potential impact on the data subject/s.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the applicable staff member’s contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. We expect everyone to share in the responsibility of maintaining an air of data protection across all aspects of the School. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Staff / data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information

is used by the School to the Bursar, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Bursar and Compliance in the first instance, and at as early a stage as possible, and usually at least half a term in advance of planned use.

Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Bursar as soon as possible.

The time limit for a response to a subject access request starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. This means that if the request was received on 20 August 2024, the school should respond by 19 September 2024 (not 20 September).

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. For example if you receive a request on 31 March. The time limit starts from the same day. As there is no equivalent date in April, you will have until 30 April to comply with the request.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond. So if a request is received on 25 November, you have until 27 December to respond (25 and 26 December being bank holidays).

A subject access request does not even have to be in writing – it can be made orally, to any member of staff, at any time.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

- None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and
- object to direct marketing; and
- withdraw their consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Bursar as soon as possible.

Data Security: Online and Digital

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.

All staff must comply with the School's Acceptable Use Policy and E-Safety Policy. In short, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar. Where a worker is permitted to take data offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.

The NCSC emphasises that passwords should not be re-used across accounts and encourages the use of multi-factor authentication (MFA).

Processing of Financial or Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details), may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

Biometric Data

The School does not process biometric data, except in accordance with Clause 3.5 of the Parent Contract and except for voluntarily consenting to using the Face ID or Touch ID feature on school-issued iPads for security purposes.

Further information can be found at https://support.apple.com/en-gb/guide/security/sec067eb0c9e/1/web/1 regarding these features, and such information may be updated from time to time.

Other biometric data

Increasingly, some schools use simple biometrics (e.g. fingerprinting or facial recognition) to enable security measures on school premises: from door or gate access, or log-ins to devices (e.g. library services), through to local uses such as lockers or payment for (where applicable) lunches/ snacks. This technology is becoming more widely available and has benefits for security and safeguarding, as well as efficiencies. We have not adopted the use of simple biometrics.

To process biometric data, the School would need written consent from at least one parent for all pupils under the age of 18 (that would be sought out separately) to comply with Protection of Freedoms Act 2012. The School would also need to comply with the Data Protection Act 2018 for biometric data collected. Schools are simply not allowed to collect any biometric data until they have written parental consent, except in extreme and unusual circumstances. Although schools do not need to have written consent from the pupil, we would need to respect pupils' wishes if they refuse to participate. A pupil's objection will always override parental consent in this regard, and indeed the objection of one parent can override the consent of another. Consent may also be withdrawn at any stage. In addition, "reasonable alternative arrangements" must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate. The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services / school premises etc. as a result of their not participating. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Queries

Any comments or queries on this policy should be directed to one of the POs using the following contact details:

Deputy Head Teaching & Learning: 020 7720 4091 extn 1224 Email nstone@newtonprep.co.uk

Head of Digital Learning: 0202 720 4091 extn 1243 Email odobbing@newtonprep.co.uk

Bursar: 020 7720 4091 extn 1204 Email: bursar@newtonprep.co.uk

Data Manager: 020 7720 4091 extn 138 Email: datamanager@newtonprep.co.uk

Compliance Officer: 0207 720 4091 extn 1206 Email compliance@newtonprep.co.uk

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the POs.

Accessing the Policy: This policy is also available in various formats to allow everyone to access it Please contact the Bursar to request a copy of this policy in an alternative form.

Review and Update Process

Last update	September 2024
Next update	September 2025