

The Birches Specialist Support School Data Protection, GDPR and Freedom of Information Policy



Date Reviewed: March 2019

Reviewed by: A White School Business Manager
Supported by C Cassidy Governor & F Shah Deputy Headteacher

**The Finance, Premises & Personnel Committee on behalf of the
Governing Body**

Signed:.....
On behalf of the Governors

Signed:
Head teacher

Date of next review: February 2021

Contents

- 1. Introduction**
- 2. Scope**
- 3. Data Protection Act 2018**
- 4. Dealing with Rights of Access and GDPR**
- 5. The Freedom of Information Act 2000**
- 6. Dealing with a request under the Freedom of Information Act**
- 7. Complaints**
- 8. Further Advice and Information**

1. Introduction

- 1.1 The school collects a large amount of personal data including: pupil records, staff records, names, and addresses of those requesting prospectuses, references, fee collection, as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

From 25 May 2018, the General Data Protection Regulation (GDPR) as supplemented by the UK Data Protection Act 2018 took legal effect.

This replacement data protection framework places new obligations on organisations and strengthens the rights that individuals have over the processing of their personal information.

These rights are as follows;

- the right to be informed;
- to ask us for access to copies of the personal information we hold about you;
- to ask us to rectify your personal information if it is inaccurate or incomplete;
- to ask us to stop processing your personal information (this is known as the 'right to object');
- to ask us to erase personal information we hold about you (this is also known as the 'right to be forgotten');
- to ask us to 'restrict' the processing of your personal information (e.g. restrict our access and use pending our consideration, for example, of any objection or erasure request you have submitted);
- to ask us ensure that a decision which legally affects you is reviewed by a person if the decision has been made solely using an automated computerised process;
- to ask us to put the personal information you have given us into a portable electronic machine readable format so it is capable of being transmitted to someone else.

Please be aware that these rights are not absolute and are subject to conditions and exemptions. In some cases the rights described above only apply if the processing activity is undertaken on specific legal grounds and/or in defined circumstances. Therefore all of these rights are unlikely to be engaged in all cases.

Full information about individual's rights can be found on the Information Commissioner's Office (the ICO) website. The ICO is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under data protection law.

1.2 Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

1.3 This policy and procedure explains the duties and responsibilities placed on the school under the legislation relating to data protection issues to ensure that all data is handled and stored securely. The document also explains the processes available to individuals to access information held by the school.

2. Scope

2.1 This policy relates to all employees, volunteers, contractors, pupils and parents. It also explains how members of the public may request information held by the school.

3. Data Protection Act 2018

3.1 The Data Protection Act describes how organisations must collect, handle, and store personal information. The rules apply regardless of whether the data is stored electronically, on paper or in other formats.

3.2 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.3 The Data Protection Act 2018 is underpinned by important principles.

These state that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

3.4 To comply with the Data Protection Act the school must:

- Manage and process personal data properly
- Protect the individuals' right to privacy
- Provide an individual with access to all personal data held on them.

3.5 The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the **Data Controller** under the Act.

3.6 Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.7 Every member of staff that holds personal information has to comply with the Act when managing that information.

3.8 The school is committed to maintaining the eight principles at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it, and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and **legally appropriate to do so**
- set out clear procedures for responding to applications for access to personal information known as Subject Access requests in the Data Protection Act (**see paragraph 4**)
- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

4. Dealing with Rights of Access and GDPR

4.1 Any individual, including members of staff, parents and pupils, has the right of access to information held about them. However with children, this is dependent upon their capacity to understand. A child is expected to be mature enough to understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf. We would need to be satisfied of parental responsibility in all cases.

4.2 Requests for personal information must be addressed to the school. If the initial request does not clearly identify the information required, then further clarification may be sought from the enquirer. The school office must keep a record of all requests made whether verbally, in writing or through social media.

4.3 The response time for Subject Access requests, once officially received, is one calendar month, irrespective of school holiday periods.

Example 1

The school receives a request on 3 September. The time limit will start from the next day (4 September). This gives the school until 4 October to comply with the request.

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.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example 2

The school receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the school has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if;

- it is manifestly unfounded or excessive
- an exemption applies; or
- you are requesting proof of identity before considering the request.

4.4 There are some exemptions to the right to Subject Access data that apply in certain circumstances or to particular types of personal information. The following examples are provided for indicative purposes only and are not intended to be exhaustive:

- Responding to a request may involve providing information relating to another individual (a third party). Third party information is that which identifies another pupil/parent or has been

provided by another agency, such as the Police, Local Authority, Health Care Professional, or another school. Before disclosing third party information consent should normally be obtained. There is still however a need to adhere to the one calendar month statutory timescale and also the information under 'Can we extend the time for a response?' as above.

- Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

4.5 In certain circumstances it may be appropriate to provide redacted (information edited or removed) to protect the legal rights of named individuals or agencies.

4.6 Therefore all information must be reviewed prior to disclosure. Where there are concerns over the disclosure of information then appropriate professional advice should be sought where necessary.

4.7 Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

4.8 Information can be viewed at the school with a member of staff on hand to help and explain matters if requested, or provided at a face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

GDPR

The school will ensure that personal data is protected and kept safely and securely.

It will ensure that its policy for data protection is used as the basis for collecting, storing, accessing, sharing and deleting personal data. The school will use the General Data Protection Regulations (GDPR) as the benchmark for its standard for protecting personal data.

Objectives

1. To ensure that decision makers and key people in school comply with the statutory changes to the GDPR in which came into force on 25 May 2018.
2. To ensure that there will be regular reviews and audits of the information we hold to ensure that we fully meet the GDPR statutory requirements.
3. To document the personal data we hold, where it came from and with whom it will be shared.
4. To ensure that data collection, data handling, data storage and data disposal procedures are in line with the GDPR and cover all the rights individuals have, including how personal data is deleted and destroyed.

Strategies

1. Data access request procedures will be handled within the timescales set out in the GDPR and we provide any additional information in line with the GDPR guidance.
2. The processing of personal data will be carried out on a lawful basis as required by the GDPR.
3. Where the school needs to seek consent, it will do so in a manner that meets GDPR standards.
4. Any records of consent and the management of the process for seeking consent will also meet the GDPR standard.
5. Where there is a personal data breach the procedures used to detect, report and investigate it will meet the requirements of the GDPR.
6. The systems the school puts into place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity will meet the standard set in the GDPR.
7. Data protection by design and data protection impact assessments will meet with the ICO's code of practice on privacy impact assessments as well as with the latest guidance.
8. There will be a data protection liaison officer for the external DPO provider – Manchester City Council.
10. When the school requests data we will provide appropriate privacy notices to explain why data is being and the purposes for which it is used.

Outcomes

The requirements of the GDPR will be met by this school as the basis for collecting, storing, accessing, sharing and deleting personal data. Data will be processed fairly lawfully and in a transparent manner. It will be used for specified, explicit and legitimate purposes in a way that is adequate, relevant and limited. It will be accurate and kept up to date and kept no longer than is necessary. Data will be processed in a manner that ensures appropriate security of the data.

5. The Freedom of Information Act 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- Public authorities are obliged to publish certain information about their activities; and
- Members of the public are entitled to request information from public authorities.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves). If a member of the public wants to see information that a public authority holds about them, they should make a Subject Access Request under GDPR.

Anyone can make a freedom of information request – they do not have to be UK citizens, or resident in the UK. Freedom of information requests can also be made by organisations, for example a newspaper, a campaign group, or a company.

Employees of a public authority can make requests to their own employer, although good internal communications and staff relations will normally avoid the need for this.

Please note that reference in the Freedom of Information Act 2000 to “public authorities” applies to all publically funded schools and academies.

6. Dealing with a request under the Freedom of Information Act

Any letter or email to the school asking for information is a request for recorded information under the Act, although it may be more appropriate to deal with routine requests for information in accordance with normal procedures.

The provisions of the Act need to come into force only if:

- The school cannot provide the requested information straight away; or
- The requester makes it clear they expect a response under the Act.

For a request to be valid under the Freedom of Information Act it must be in writing (includes email) and include a real name and address to reply to, however requesters do not have to mention the Act or direct their request to a designated member of staff.

From the ICO website;

'What are the legal requirements for a request?'

For your request to be dealt with according to the Freedom of Information Act, you must:

- *contact the relevant authority directly;*
- *make the request in writing, for example in a letter or an email. You can make a verbal or written request for environmental information;*
- *give your real name; and*
- *give an address to which the authority can reply. This can be a postal or email address.*

*You do **not** have to:*

- *mention the Freedom of Information Act or Environmental Information Regulations, although it may help to do so;*
- *know whether the information is covered by the Freedom of Information Act or the Environmental Information Regulations; or*
- *say why you want the information.*

It is sensible to write the date on any letters or emails you send and keep a copy, so you have a reliable record of your request. If you make a verbal request for environmental information, we recommend that you note who you spoke to, the date, and what information you requested, and you may wish to follow up with a letter or email confirming your request. A written record of a verbal request would be beneficial if you later need to make a complaint.

It can be helpful to check whether the authority recommends you send your request to a specific person or email address. Some authorities allow you to request information via their website. You can also make a request on social networking sites such as Facebook or Twitter.

Some other websites allow you to contact public authorities and make a request through the site. Check that the site will allow the public authority to respond, otherwise it's not a valid request.

If you find it impossible or unreasonably difficult to make a request in writing, a public authority may have to make a reasonable adjustment for you under the Equality Act 2010 (or Disability Discrimination Act 1995 in Northern Ireland). This could mean, for example, that the public authority has to consider treating a verbal request for information as if it was a valid freedom of information request.

The ICO cannot request information from another authority on your behalf. You should address your request directly to the authority.' <https://ico.org.uk/your-data-matters/official-information/>

The school has two separate duties when responding to these requests:

- to tell the applicant whether they hold any information falling within the scope of the request;
- and
- to provide that information

In accordance with the Act the school will normally respond to the request within 20 working days.

The school may refuse to provide information requested under the Act in the following limited circumstances;

- It would cost too much or take too much staff time to deal with the request – this is limited to a cost of £450 and 18 hours of staff time.
- The request is vexatious - instituted without sufficient grounds and serving only to cause annoyance to the defendant.
- The request repeats a previous request from the same person.

In addition, the Freedom of Information Act contains a number of exemptions that allow you to withhold information from a requester. In some cases it will allow you to refuse to confirm or deny whether you hold information.

Some exemptions relate to a particular type of information, for instance, information relating to government policy. Other exemptions are based on the harm that would arise or would be likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests.

There is also an exemption for personal data if releasing it would be contrary to the Data Protection Act. You can automatically withhold information because an exemption applies only if the exemption is 'absolute'. This may be, for example, information you receive from the security services, which is covered by an absolute exemption. However, most exemptions are not absolute but require you to apply a public interest test. This means you must consider the public interest arguments before deciding whether to disclose the information. So you may have to disclose information in spite of an exemption, where it is in the public interest to do so.

If you are refusing all or any part of a request, you must send the requester a written refusal notice. You will need to issue a refusal notice if you are either refusing to say whether you hold information at all, or confirming that information is held but refusing to release it.

Before refusing to provide any information requested, the school should consult the Information Commissioner's Office website at www.ico.gov.uk for more information.

7. Complaints about data protection, GDPR and Freedom of Information

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's Compliments and Complaints Policy.

The first step would be an internal review of the complaint by the most relevant person in school and someone who is more senior than the original decision maker.

Complaints which are not appropriate to be dealt with through the school's Compliments and Complaints Policy and procedure can be dealt with by the Information Commissioner.

8. Further Advice and Information

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Additional Information below from the ICO website
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

What about requests for large amounts of personal data?

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.

You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when you receive the additional information. However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request ie by making reasonable searches for the information covered by the request.

What about requests made on behalf of others?

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of

an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters:

- *in England and Wales, by the Court of Protection;*
- *in Scotland, by the Sheriff Court; and*
- *in Northern Ireland, by the High Court (Office of Care and Protection).*

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- *the child's level of maturity and their ability to make decisions like this;*
- *the nature of the personal data;*
- *any court orders relating to parental access or responsibility that may apply;*
- *any duty of confidence owed to the child or young person;*
- *any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;*
- *any detriment to the child or young person if individuals with parental responsibility cannot access this information; and*
- *any views the child or young person has on whether their parents should have access to information about them.*

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

Policy Information and Review

Review frequency: every 2 years

Date	Version	Changes made	By whom (name and role)	Due date for next review	Reviewed & Ratified by Govs. (sign and date)
June 2017	V1	None – adopted OneEd policy	A White SBM	June 2019	
July 2018		<p><i>Data Protection Act 2018 & GDPR added in to this policy.</i></p> <p><i>06/07/18 The Policy Ratification Committee has met and requested that all current statutory policies are ratified for one year only whilst an appropriate cycle of ratification is implemented. Policies will then be approved for their full length of term either through the Full Governing Body or one of the committees following an agreed plan of ratification.</i></p>			
February 2019	1	Dates changed for ratification purposes – policy is the same just the dates altered	F Shah DHT	February 2021	
18/03/2019	2	Policy updated based on DP Act 2018 and GDPR, rights of access and examples included with ref to ICO website	F Shah DHT With support from C Cassidy Governor	February 2021	