

BRIGHT FUTURES 4 ALL



GDPR & DATA PROTECTION POLICY

Ratified: September 2024

Review: September 2025

Bright Futures 4 All – GDPR & Data Protection Policy

CONTENT

1. Introduction
2. Personal Data
3. The Data Protection Principles
4. Conditions for Processing in the First Data Protection Principle
5. Use of Personal Data by the Education service
6. Security of Personal Data
7. Disclosure of Personal Data to Third Parties
8. Confidentiality of Student Concerns
9. Subject Access Requests
10. Exemptions to Access by Data Subjects
11. Other Rights of Individuals
12. Breach of Any Requirement of the GDPR
13. Contact



FREEDOM OF INFORMATION

1. Introduction
2. What is a Request under FOI
3. Time Limit for Compliance
4. Procedure for Dealing with a Request
5. Responding to a Request
6. Contact

DATA PROTECTION

INTRODUCTION

Bright Futures 4 All exists as a distinct education service community because it has Christ's teachings as its foundation. His teaching and example are the basis for its daily life, relationships and future hopes. It should be possible to meet Christ in all aspects of the life of the education service and the spiritual dimension should underpin all its work.

Bright Futures 4 All collects and uses certain types of personal information about staff, students, parents and other individuals who contact the education service to provide education and associated functions. The education service may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every year.

PERSONAL DATA

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- Genetic or biometric data for the purpose of uniquely identifying a natural person.
- Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The education service does not intend to seek or hold sensitive personal data about staff or students except where the education service has been notified of the information, or it comes to the education service's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of



good practice. Staff or students are under no obligation to disclose to the Education service their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

THE DATA PROTECTION PRINCIPLES

The six data protection principles as laid down in the GDPR are followed at all times:

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the education service is committed to ensure that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 & 8 below):

The education service is committed to complying with the six data principles at all times. This means that the education service will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests;
- Report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
3. The processing is necessary for the performance of a legal obligation to which we are subject.
4. The processing is necessary to protect the vital interests of the individual or another.
5. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.



The processing is necessary for a legitimate interest of the education service or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

USE OF PERSONAL DATA BY THE EDUCATION SERVICE

The education service holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3 above.

Students

The personal data held regarding students includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the education service performs, together with any other uses normally associated with this provision in an education service environment.

The education service may make use of limited personal data (such as contact details) relating to students, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with students of the education service, but only where consent has been provided to this.

In particular, the education service may:

- transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the education service but only where consent has been obtained first
- make personal data, including sensitive personal data, available to staff for planning curricular or extracurricular activities;
- keep the student's previous education provider informed of their academic progress and achievements e.g. sending a copy of the academic reports for the student's first year at the education service to their previous education provider;
- Use photographs of students in accordance with the photograph policy.

Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer in writing, which notice will be acknowledged by the education service in writing. If, in the view of the Data Protection Officer, the objection cannot be maintained, the individual will be given written reasons why the education service cannot comply with their request.

Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

The data is used to comply with legal obligations placed on the education service in relation to employment, and the education of children in an education service environment. The education service may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Personnel Officer who will ensure that this is recorded, and adhered to if appropriate. If the Personnel



Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual would be given written reasons why the education service cannot comply with their request.

Other Individuals

The education service may hold personal information in relation to other individuals who have contact with the education service, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

SECURITY OF PERSONAL DATA

The education service will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The education service will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

For further details as regards security of IT systems, please refer to the ICT Policy.

DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

The following list includes the most usual reasons that the education service will authorise disclosure of personal data to a third party:

1. To give a confidential reference relating to a current or former employee, volunteer or student;
2. for the prevention or detection of crime;
3. for the assessment of any tax or duty;
4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation imposed by contract);
5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
6. for the purpose of obtaining legal advice;
7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
8. to publish the results of public examinations or other achievements of students of the Academy;
9. to disclose details of a student's medical condition where it is in the student's interests to do so,
10. for example for medical advice, insurance purposes or to organisers of education service external trips;
11. to provide information to another educational establishment to which a student is transferring;
12. to provide information to the Examination Authority as part of the examination process; and
13. To provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them.

On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.



The education service may receive requests from third parties (i.e. those other than the data subject, the education service, and employees of the education service) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allows disclosure applies; or where necessary for the legitimate interests of the individual concerned or the education service.

All requests for the disclosure of personal data must be sent to Data Protection Lead who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

CONFIDENTIALITY OF STUDENT CONCERNS

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the education service will maintain confidentiality unless:

- it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent;
- or where the education service believes disclosure will be in the best interests of the student or other students

Please see the Safeguarding and Student Protection Policy for further details

SUBJECT ACCESS REQUESTS

Under Data Protection Law, Data Subjects have a general right to find out whether the education service hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the education service are undertaking.

A Data Subject has the right to be informed by the education service of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the education service's sources of information obtained;
- (g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision-making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
- (h) Other supplementary information.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their daughter): for confirmation as to whether the education service process personal data about him or her and, if so

- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request.



For example, a letter which states 'please provide me with a copy of information that the education service holds about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the education service to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request that may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to Mrs Kulka, Business Manager who will contact Judicium as DPO in order to assist with the request and what is required.

Acknowledging the request

When receiving a SAR the education service will acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request. In addition to acknowledging the request, the education service may ask for: - proof of ID (if needed); - further clarification about the requested information; - if it is not clear where the information shall be sent, the education service must clarify what address/ email address to use when sending the requested information; and/or - consent (if requesting third party data).

The education service should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the education service will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The education service is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the education service has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement. If an individual is requesting a large amount of data the education service may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The education service shall let the requestor know as soon as possible, where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the education service does not receive this information, it will be unable to comply with the request.

Requests made by third parties or on behalf of children

The education service needs 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. The education service may also require proof of identity in certain circumstances.

When requests are made on behalf of students, it is important to note that even if a student is too young to understand the implications of subject access rights, it is still the right of the student, rather than of anyone else such as a parent or carer, to have access to the student's



personal data. Before responding to a SAR for information held about a student, the education service should consider whether the student is mature enough to understand their rights. If the education service is confident that the student can understand their rights, then the education service should usually respond directly to the student or seek their consent before releasing their information.

It shall be assessed if the student 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, it should be taken into account, among other things:

- the student'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 student or young person;
- any consequences of allowing those with parental responsibility access to the students or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the student or young person if individuals with parental responsibility cannot access this information; and
- any views the student or young person has on whether their parents should have access to information about them.

Generally, 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. In relation to a student 12 years of age or older, then provided that the education service is confident that they understand their rights, and there is no reason to believe that the student does not have the capacity to make a request on their own behalf, the education service will require the written authorisation of the student before responding to the requester, or provide the personal data directly to the student.

The education service may also refuse to provide information to parents if there are consequences of allowing access to the student's information – for example if it is likely to cause detriment to the student.

Fee for responding to a SAR

The education service will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive, a fee to cover administrative costs may be requested.

Time Period for Responding to a SAR

The education service has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received. The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the education service will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

Education service closure periods

Requests received during or just before education service closure periods may not be able to be responded to within the one calendar month response period. This is because the education service may be closed or no one will be on site to comply with the request.



As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time; however, if we can acknowledge the request we may still not be able to deal with it until the education service re-opens. The education service will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during or close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her. The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the education service is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the education service has one month in which to respond the education service is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The education service is therefore allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The education service is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the education service needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

EXEMPTIONS TO ACCESS BY DATA SUBJECTS

Protection of third parties -exemptions to the right of subject access There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case-by-case basis. The education service will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the education service do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.



It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the education service disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the education service must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the education service may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The education service does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The education service does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service.

This exemption does not apply to confidential references that the education service receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the education service must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The education service does not have to disclose any personal data, which are subject to legal professional privilege.

Management forecasting: The education service does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The education service does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

OTHER RIGHTS OF INDIVIDUALS

The education service has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the education service will comply with the rights to:

1. object to Processing;
2. rectification;
3. erasure; and
4. data Portability.

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (under Conditions for Processing in the First Data Protection Principle grounds 5 and 6 above) where they do not believe that those grounds are made out.



Where such an objection is made, it must be sent to The Headteacher within 2 working days of receipt, and The Headteacher will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The Headteacher shall be responsible for notifying the individual of the outcome of their assessment within 15 working days of receipt of the objection.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to The Headteacher within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under complaints procedure, or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
2. where consent is withdrawn and there is no other legal basis for the processing;
3. where an objection has been raised under the right to object, and found to be legitimate;
4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
5. where there is a legal obligation on the education service to delete.

The Headteacher will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

For further details please refer to Records Retention Policy.

Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

1. where the accuracy of data has been contested, during the period when the education service is attempting to verify the accuracy of the data;
2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
4. where there has been an objection made under para 8.2 above, pending the outcome of any decision.



Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that the education service provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the education service is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to The Headteacher within 2 working days of receipt, and The Headteacher will review and revert as necessary.

BREACH OF ANY REQUIREMENT OF THE GDPR

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to Data Protection Lead (Business Manager) or the Data Protection Officer (Judicium) dataservices@judicium.com

Once notified, the Data Protection Officer shall assess:

1. the extent of the breach;
2. the risks to the data subjects as a consequence of the breach;
3. any security measures in place that will protect the information;
4. any measures that can be taken immediately to mitigate the risk to the individuals.

Unless Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the education service, unless a delay can be justified.

The Information Commissioner shall be told:

1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;
2. the contact point for any enquiries (which shall usually be the Data Protection Officer);
3. the likely consequences of the breach;
4. measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

1. the nature of the breach;
2. who to contact with any questions;
3. measures taken to mitigate any risks.

The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Governing Body and a decision made about the implementation of those recommendations.

CONTACT

If anyone has any concerns or questions in relation to this Policy they should contact the Business Manager



FREEDOM OF INFORMATION INTRODUCTION

Bright Futures 4 All exists as a distinct education service community because it has Christ's teachings as its foundation. His teaching and example are the basis for its daily life, relationships and future hopes. It should be possible to meet Christ in all aspects of the life of the education service and the spiritual dimension should underpin all its work. The attitudes and values of the education service are those of Christ's radical command to love one another as I have loved you (Jn 13:34), where this love means putting others first (Mk 9:35), turning the other cheek (Mt 5:39), and going the extra mile (Mt 5:41).

St Philomena's recognises its duty to provide a safe, healthy, working environment influenced by the ethos of the education service. It believes all members within its community (governors, staff and volunteers) are its most important asset in delivering quality services to the local community and places a high value on their physical, mental and spiritual well-being.

The education service is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such must comply with any requests for information in accordance with the provisions of the Act.

WHAT IS A REQUEST UNDER FOI

Any request for any information from the education service is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Headteacher.

All other requests should be referred in the first instance to the Headteacher who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

TIME LIMIT FOR COMPLIANCE

The education service must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For an education service, a "working day" is one in which students are in attendance, subject to an absolute maximum of 60 calendar days to respond.

PROCEDURE FOR DEALING WITH A REQUEST

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Headteacher who may reallocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether or not the education service "holds" the information requested. The education service will hold the information if it exists in computer or paper format. Some requests will require the education service to take information from different sources and manipulate it in some way. Where this would take minimal effort, the education service is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request.



For example, if a request required the education service to add up totals in a spread sheet and release the total figures, this would be information “held” by the education service. If the education service would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information “held” by the education service, depending on the time involved in extracting the information. The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

1. Section 40 (1) – the request is for the applicant’s personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy above;
2. Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;
3. Section 41 – information that has been sent to the education service (but not the Education service’s own information) which is confidential;
4. Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;
5. Section 22 – information that the education service intends to publish at a future date;
6. Section 43 – information that would prejudice the commercial interests of the Education service and / or a third party;
7. Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
8. Section 31 – information which may prejudice the effective detection and prevention of crime –
9. such as the location of CCTV cameras;
10. Section 36 – information which, in the opinion of the Chair of Governors of the Education service, would prejudice the effective conduct of the education service. There is a special form for this on the ICO’s website to assist with the obtaining of the chair’s opinion.

The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

RESPONDING TO A REQUEST

When responding to a request where the education service has withheld some or all of the information, the education service must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

The letter should end by explaining to the requestor how they can complain – either by reference to complaints procedure or by writing to the ICO.

CONTACT

Any questions about this policy should be directed in the first instance to the Business Manager.

^[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.