DATA PROTECTION and FREEDOM of INFORMATION POLICY

This policy has been approved and adopted by the Christus Catholic Trust across all their academies and it will apply to all staff within the Trust.

This Policy will take effect from:	Immediate
It was adopted by the Trust Board on:	September 2021
Monitored and reviewed by:	September 2023

The Christus Catholic Trust wishes to build a welcoming community of faith that has Christ at the centre, where all within our schools' communities have a love of God and a love of one another. Prayer and liturgy will shape our daily life.

Contents

1. Aims

The Christus Catholic Trust ('the Trust') aims to ensure that all personal data collected about staff, pupils, parents, governors, directors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust and each academy within the Trust process personal data relating to parents, pupils, staff, governors, directors, visitors and others, and therefore are data controllers.

The Trust and each academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board of Directors

The Trust Board of Directors has overall responsibility for ensuring that the Trust and each academy complies with all relevant data protection obligations.

5.2 Local Governing Committees

The local governing committee has overall responsibility for ensuring that their academy complies with all relevant data protection obligations.

5.3 Data Protection Officer

Each academy will appoint a data protection officer (DPO) who is responsible for overseeing the implementation of this policy and monitoring compliance with data protection law. They will provide an annual report of their activities directly to the local

governing committee and, where relevant, report to the Trust DPO for advice and recommendations on school data protection issues.

The Trust DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They are also the first point of contact for each academy DPO, and for the ICO.

The DPO for the Trust will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The interim DPO for the Trust is Stephen Foster and may be contacted at DPO@christus.org.uk

5.4 Trust CSEL

The Catholic Senior Executive Leader (CSEL) acts as the representative of the data controller for the Trust on a day-to-day basis.

5.5 Headteacher

The Headteacher/Executive Headteacher of each academy acts as the representative of the data controller on a day-to-day basis.

5.6 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust and/or academy of any changes to their personal data, such as a change of address
- Contacting the Academy DPO (or for central staff the Trust DPO) in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that the Trust and each Academy must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust and each Academy aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust and each Academy can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust and each Academy can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust and each Academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust and each Academy or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 years of age (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent, where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must

ensure it is deleted or anonymised. This will be done in accordance with the Trust's Record Management Policy.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests (SAR) and Other Rights of Individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy or Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the Academy DPO (for central staff the Trust DPO).

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case- by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed

to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

It is expected that academies will be closed during school holidays, and therefore delays may be incurred should subject access requests be sent directly to the school. In such circumstances, requests will be passed to the DPO as soon as is practicably possible after the school holidays, and will be dealt with within one month of receipt by the DPO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO (for central staff the Trust DPO).

10. Parental Requests to See the Educational Record

There is no automatic parental right of access to the educational records in an academy setting. However, parents/carers may make a request to the school in writing to receive a copy of their child's educational record. All requests will be considered on an individual basis and reasonable fees may be charged to cover the cost of production of records.

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child *(Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18)* first takes part in it. The academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

CCTV may be used in various locations around an academy's site to ensure it remains safe. Where CCTV is in place, we will adhere to the ICO's code of practice for the use of CCTV. Although it is not necessary to gain individuals' permission to use CCTV, academies will make it clear where individuals are being recorded. Security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about individual academies' CCTV systems should be directed to the relevant academy office.

13. Photographs and Videos

As part of the Trust and each academy's activities, photographs and record images of individuals may be taken within our individual academies.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within an academy/ Trust on notice boards and in school/ Trust magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust/academies website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified, unless we have gained specific consent to do so, for example, when reporting on Awards Ceremonies. Further information on how individual academies use photographs and/or videos can be obtained from the relevant academy.

Photographs/videos taken by parents/carers at school events are done so for personal use and are not covered by the Data Protection Act 2018 (GDPR). We respectfully ask that parents/carers consider the privacy rights of individuals when taking photos or videos of children other than their own (even if pictured in the background), particularly if these are to be uploaded to social media sites or other outlets.

14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the Trust and each academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Trust, academy, academy DPO and Trust DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are securely stored when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust and school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption is used to protect all portable devices and removable media, such as laptops
- Staff, pupils, governors and directors who store personal information on their personal devices are expected to follow the same security procedures as for Trust and each academy-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where it cannot or does not need to be rectified or updated. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust/academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust and each academy will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the procedure set out in appendix 1 will be followed

When appropriate, the data breach will be reported to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the academy's website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Trust/academy laptop containing non-encrypted personal data about pupils or staff

18. Training

All staff, governors and directors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust/academy's processes make it necessary.

19. Monitoring Arrangements

The Trust DPO is responsible for monitoring and reviewing this policy which will be reviewed **every 2 years**.

20. The Freedom of Information Act

20.1 To be read in conjunction with the Christus Catholic Trust Freedom of Information Act 2000 Publication Scheme

20.2 This Act gives a general right of access to all types of 'recorded' information held by the Trust. Under this Act the Trust has two main responsibilities.

- A written guide available which displays the information that is held
- Respond to individual requests for information

20.3 The Act states that all requests for information must be made in writing to us. We will accept these in the following forms: -

- Letter
- Email

20.3 The following information must be included

- The requestor's full name
- An address for correspondence, (this can be a postal or email address)
- A clear description of the information required.

20.4 We will respond to requests for information within 20 school days. If further clarification is required, our staff will write to the requestor and the request will be temporarily placed on hold until sufficient information is available to begin processing the request

21. Review Process in regard to Freedom of Information request

21.1 Under section 45 of the Freedom of information Act a requestor can ask for a formal review of any refusal notice and/or the administration of their request. The request for a review must be made in writing and received by the Chair of Directors within 40 working days of the alleged failure to comply with the Act.

21.2 On receipt of a request to review the Chair of Directors and CSEL/AO will conduct a full assessment and aim to respond within 20 school days.

21.3 If upon following this process the requestor remains dissatisfied they should then contact the Information Commissioner's Office for advice.

22. Links with other policies

This data protection and freedom of information policy is linked to our:

- Freedom of Information Act publication scheme
- Privacy Notices, both for the Trust and its individual schools
- Code of Conduct policy
- Child Protection and Safeguarding Policies

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Headteacher/Executive Headteacher (if not DPO of academy), chair of Local Governing Committee and Trust DPO
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be kept on Trust and each academy's computer system in a designated area
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again(such as establishing more robust processes or providing further training for individuals)

    Records of all breaches will be stored in the Trust/academy's computer system in a designated area.

    The DPO and Headteacher (if not DPO of academy) and Trust DPO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will take reasonable steps to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

The school's cashless payment provider being hacked and parents' financial details stolen

- Parents will be alerted and advised to check with their bank and change passwords.
- A review of the provider's security settings will be carried out
- The provider will be expected to compensate for any loss as a result of the data breach.

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 2: Request for information under Freedom of information Act

Requests for Information

Any request for information beyond that which is already provided by the school (for example, through the schools' Prospectuses, their websites and Trust's Statutory accounts, or information about children to which parents already have access) should be made in writing (this includes email) to the Headteacher of the relevant school. Section 8 of the FOIA states any request should state the applicants name and address for correspondence and describe details of the information being requested.

If a request is very general, the school may contact the enquirer for clarification of the request. The person making the request for information can also indicate how they would like to receive the information and where possible the school will try to comply with those wishes. If it is not possible to do so, the school will notify the enquirer and offer an alternative.

Any member of staff may be approached for information beyond which may be regarded as 'normal information'. In this context, 'normal' means the kind of information that teachers and other members of school staff feel confident about giving, as opposed to requests for information which may seem of an intrusive or sensitive nature. If a member of staff receives such a request, they should avoid giving an immediate response and refer the request in the first instance to the Headteacher of the relevant school. Depending upon the nature of the request, after discussion the Headteacher may then either sanction a response or refer the request to the relevant person(s) or the appropriate level of governance.

Under the Freedom of Information Act (FOIA) the enquirer is entitled to be told whether the academy holds the information (the duty to confirm or deny) except where certain exemptions apply. The Headteacher is responsible for ensuring that all members of staff are familiar with this policy and the procedures to be adopted in responding to requests for information under the FOIA.

Responding to Requests for Information

Any requests are to be passed to the Headteacher, of the relevant school, who will, as appropriate, then pass the request on to the relevant person(s) or to the Local Governing Committee. The relevant person(s) will document any requests received and keep records of their deliberations and outcomes. The potential outcomes are:

- Agreement to meet the request in full
- Agreement to meet the request in part (with reasons)
- Refusal to meet the request (with reasons)

The relevant person(s) will respond to the enquirer within 20 school days (i.e. excluding weekends and school holidays) of the request being made. (Note: The 20 day time limit starts the day after the request has been received. The period from the day the fees notice is issued, if applicable, to the day the fee is received does not count towards the 20 working day limit for response). The response to the request in some circumstances may take longer than 20 days. If a request is delayed for any reason (if further information is required/in order to identify and locate the information requested), the enquirer will be kept informed of the progress and where possible provide an expected date for a response.

Under the FOIA 2000, certain information is exempt from disclosure. The application of Section 36 needs to be approved by a qualified person, which in this case is the Chair of the

Local Governing Committee, who will give their reasonable opinion that disclosure would or would not be likely to cause the types of prejudice or inhibition within the meaning of the FOIA 2000. [Note: further guidance on this exemption can be found at www.ico.gov.uk).

The Act states that requests should not be allowed to cause a drain on school's time, energy and finances to the extent that they negatively affect normal public functions (in excess of 3.5 days). The Trust can reserve the right to refuse a request if it is likely to be in excess of 3.5 days to find, sort and edit the information requested. Under these circumstances the Trust will provide an opportunity for the request to be refined.

Wilfully concealing, damaging or destroying information in order to avoid answering an enquiry is an offence. Any expressions of dissatisfaction with the information provided or the decision to refuse to supply information by the Appeals Committee should then be addressed to the Information Commissioner's Office (ICO).

Vexatious Requests

Under section 14 of the FOIA if schools receive several requests from the same person, or a series of requests that the schools think are intended to disrupt their work, these may be treated as repeated or vexatious. In this case the Trust may refuse to provide the information requested but would issue a refusal notice within 20 school days from receipt of the request to the enquirer to explain the decision and reasons for withholding the information (Note: this must include information regarding the appeals process).

Appeals

Upon notification of a refusal to meet the request (either in part or in whole), the party making the request for information may appeal the decision. Any such appeal will be considered by the Trustees of the Trust. If the enquirer is still not satisfied with the outcome they can commence the complaints process to the ICO.

Use of Information Provided

The Freedom of Information Act allows access to information, but it does not give the enquirer permission to re-use that information for commercial gain. Therefore, the enquirer may reproduce the Trust's copyright protected information free of charge, without specific permission, provided it is not being reproduced for profit, material or financial gain. The material must be reproduced accurately and must not be used in a misleading context. If the enquirer is publishing the material or issuing it to others, they must acknowledge the source of the information, its copyright status and the date of publication, if known. This permission to reproduce the school's copyright protected material does not extend to any material that is identified as being the copyright of a third party. Under those circumstances, the enquirer must seek authorisation to reproduce the material from the copyright holder concerned.

Appendix 3: Checklist for action on receipt of a request under Freedom of information

Checklist

- Decide whether the request is a request under DPA (Data Protection Act 1998), EIR (The environmental information regulations 2004) or FOIA (The Freedom of Information Act 2000)
- Decide whether the school/Trust holds the information or whether it should be transferred to another body
- Provide the information if it has already been made public
- Inform the enquirer if the information is not held
- Consider whether a third party's interests might be affected by disclosure and if so consult them
- Consider whether any exemptions apply and whether they are absolute or qualified
- Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information
- If a request is made for a document that contains exempt personal information ensure that the personal information is removed as set out in guidance
- Decide whether the estimated cost of complying with the request will exceed the appropriate limit
- Consider whether the request is vexatious or repeated
- Update records

Record Keeping

- Records will be entered into a "Freedom of Information Requests Log" kept within each school. Such records will remain on file for a period of six years and will be disposed of at a set time in a calendar year.
- The log will include details of:
    - The party making the request for information
    - The date upon which the request was received (date stamp) and to whom it was addressed
    - If relevant, the date upon which the request was subsequently referred (internal/external)
    - The nature of the information requested
    - The date and time of any meeting(s) convened to consider the request
    - The outcome of any deliberations, including summary reasons for any refusal (in whole or in part) to meet the information request
    - The response made to the party requesting the information, including the person nominated to implement
    - The response (Headteacher or other) the date and format of the response and the details of the information provided.
    - Any subsequent appeal made by the enquirer
    - The outcome of the appeals process, including summary reasons for a refusal (in whole or in part) to meet the information request
    - The response to the party making the appeal, including the person nominated to implement the response,
    - the date and format of the response and the details of the information provided.
    - The appeals process shall be conducted without reference to the records of the original meeting at which the request for information was refused.