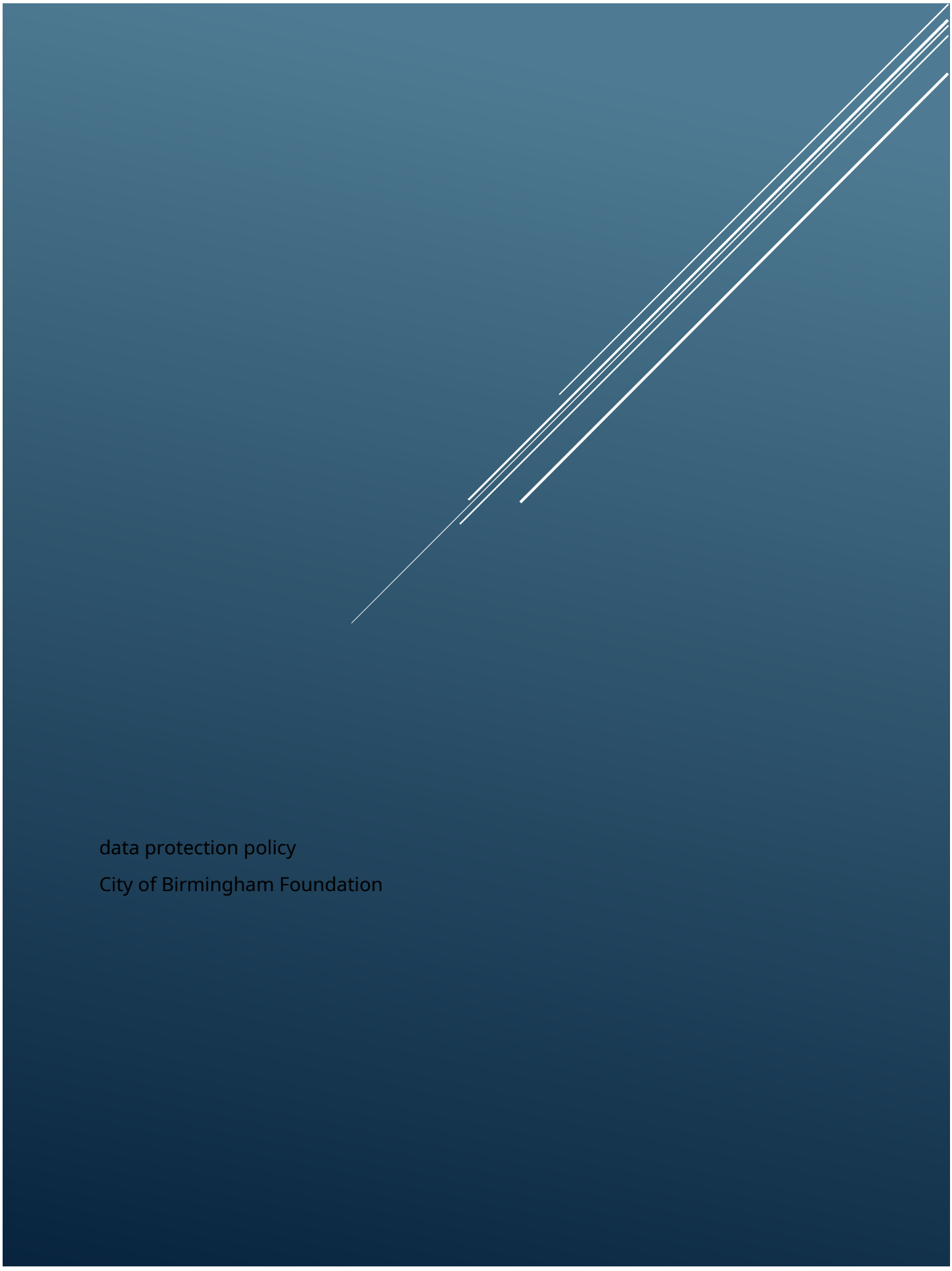

data protection policy

City of Birmingham Foundation

City of Birmingham Foundation

Contents

1. Background....2
2. Aims....3
3. The Trust's Operating Norms....3
4. Legislation and Guidance....4
5. What is Personal Information?....4
6. Roles and responsibilities....4
7. Data Protection Principles....6
8. Policy Statement....6
9. Lawful Processing....7
10.Privacy Notices and the right to be informed....8
11.Consent....8
12.Right of access....8
13. The right to rectification....9
14. The right to erasure....9
15. The right to restrict processing....10
16. The right to data portability....11
17. The right to object....11
18.Privacy by design and privacy impact assessments....12
19. Data breaches....13
20. Data security....14
21.Publication of information....16
22.CCTV....16
23.Photography....16
24. Data retention....17

25.Record Keeping.....18

26. Training.....18

27.Subject Access Requests.....18

28. Disposal of records.....20

29.Links to other policies.....20

30.Complaints.....21

31.Contacts.....21

City of Birmingham Foundation

1. Background

CoBF and its academies collect and use personal information about staff, students, parents/carers and other individuals to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust and its academies comply with statutory obligations.

CoBF is registered, as a Data Controller, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are available on the ICO's website. All trusts and academies also have a duty to issue a Privacy Notice to all students, parents/carers, staff, volunteers and governors; this summarises the information held on individuals, why it is held and the other parties with whom it may be shared.

2. Aims

Our Trust aims to ensure that all personal data collected about staff, students, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection Law.

3. The Trust's Operating Norms

The operating norms below set out the Trust's expectation to the way that all staff are required to conduct themselves whilst at work and when representing the Trust externally.

We are CoBF: We all own the name, the right to speak, the reward and the responsibility.

We believe the best of each other, speak positively and act with thought and purpose in order to find solutions and to do good work.

The standard is excellence: Excellence is our bar, it's what we aim for together, nothing less – so we support each other to get better faster

We champion equality: Inclusion and equality are central to our mission. We aim to leave no-one behind and we are fiercely anti-discrimination.

We're in the work together: We each stand by our mission and we act with transparency and clarity.

Because we share accountability, we both give and receive feedback. We celebrate honest support that makes us collectively better.

We behave with integrity: Professionalism, honesty and humanity underpin every word and action. Truth and kindness work hand in hand. We lead by example: We own our responsibility to live our norms. We expect to be role models to those around us in matters both small and large.

We use time well: Time is precious so we work smart. We select actions that provide the most benefit from time invested. We avoid creating unnecessary work for others. By their nature, the operating norms are not exhaustive but they set out the principles to be observed.

4. Legislation and Guidance

This policy meets the requirements of the:

• UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

• Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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

It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

5. What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Examples of this would be contact details, students' education records or photographs taken at academy events.

6. Roles and responsibilities

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

Board of Trustees and the Chief Executive Officer

The Board of Trustees has overall responsibility for ensuring that our trust complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (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 will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on academy data protection issues. The DPO is also the first point of contact for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Data Protection Leads

The Date Protection Leads are responsible for supporting the drive for compliance with GDPR and ensuring the ongoing compliance of all core activities within their academies. The DPLs are the main contact at academy level and will liaise with the DPO on all GDPR matters and report to and work with the DPO on all breaches, SAR's and FOIs at their academy.

Principals

The principal acts as the representative of the data controller on a day-to-day basis.

All Staff

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the academy of any changes to their personal data, such as a change of address

• Contacting the DPL in the first instance or the 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 UK

➢ 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

7. Data Protection Principles

There are several enforceable principles that must be adhered to:

• Personal data shall be processed fairly, lawfully and in a transparent manner

• Personal data shall be collected only for one or more specified and lawful purposes and processed in a way that is compatible with those purposes

• Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

• Personal data shall be accurate and where necessary, kept up to date and every reasonable step should be taken to delete or rectify inaccurate data without delay

• Personal data in a form which permits identification of data subjects, should be kept for no longer

than is necessary; personal data may be stored for longer if this is solely for archiving purposes in the public interest, scientific, historical, research or statistical purposes subject to appropriate measures to safeguard the rights of individuals

• Personal data shall be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

8. Policy Statement

CoBF and its academies are committed to maintaining the above principles at all times. Therefore, we will:

• Inform individuals why information is being collected when it is collected via privacy notices.

• Inform individuals when their information is shared, and why and with whom it was shared via privacy notices.

• Check the quality and the accuracy of the information it holds.

• Ensure that information is not retained for longer than is necessary.

• Ensure that when obsolete information is destroyed that it is done so appropriately and securely.

• Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

• Share information with others only when it is legally appropriate to do so.

• Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.

• Ensure our staff are aware of and understand our policies and procedures.

9. Lawful Processing

We collect and use student information under Article 6, and Article 9 of the UK GDPR where data processed is a special category data and for data collection purposes under the Education Act 1996 https://www.gov.uk/education/data-collection-and-censuses-for-schools

The lawful bases for processing are set out in Article 6 of the UK GDPR. One of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process your personal data for a specific purpose

(b) Contract: the processing is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations)

(d) Vital interests: the processing is necessary to protect someone's life

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect an individual's personal data which overrides those legitimate interests.

(This does not apply to academies who are a public authority, and the processing of data is required to perform official tasks.)

10.Privacy Notices and the right to be informed

A privacy notice is a statement that describes how we use, retain and disclose personal information. Different organisations sometimes use different terms, and it can be referred to as a privacy statement, a fair processing notice or a privacy policy.

To ensure that we process your personal data fairly and lawfully we are required to inform you:

• What information we collect, hold and share

• Why we collect and use this information

• The lawful basis on which we use this information

• Who we share this information with

• Why we share this information

• Our data collection requirements

• How you can access this data and your rights

11.Consent

Where consent is required, this must be a positive action and it cannot be inferred from silence, inactivity or pre-ticked boxes. Consent forms are provided to students over the age of 12, parents/carers and staff and a record will be kept of what consent was given and when. When gaining student consent, consideration will be given to the age, maturity and mental capacity of the student in question. Consent will only be gained from students where it is deemed that the student has a sound understanding of what they are consenting to.

Consent that has been given under the Data Protection Act 1998 that fully meets the requirement of the UK GDPR will be retained.

12.Right of access

Individuals have the right to obtain confirmation that their data is being processed and to have access to the personal data to verify that the processing is lawful. This is known as a Subject Access Request. Please refer to the section entitled Subject Access Requests for further information.

13. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. We will also take the following action:

• Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible

• Where appropriate, we will inform the individual about the third parties that the data has been disclosed to

• Requests for rectification will completed within one month; this may be extended by two months where the request for rectification is complex

• Where no action is being taken in response to a request for rectification, we will explain the reason for this and will inform you or your right to complain to the Trust or the Information Commissioner

14. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

• Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

• When consent has been withdrawn

• When an individual object to the processing and there is no overriding legitimate interest for continuing the processing

• The personal data was unlawfully processed

• The personal data is required to be erased to comply with a legal obligation

• The personal data is processed in relation to the offer of information society services to a child

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

• To exercise the right of freedom of expression and information of the Academy or Trust

• To comply with a legal obligation for the performance of a public interest task or exercise of official authority

• For public health purposes in the public interest

• For archiving purposes in the public interest, scientific research, historical research or statistical purposes

• The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and then later requests erasure of the data, regardless of their age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

15. The right to restrict processing

Individuals have the right to block or suppress processing of personal data.

In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

We will restrict the processing of personal data in the following circumstances:

• Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data

• Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual

• Where processing is unlawful, and the individual opposes erasure and requests restriction instead

• Where we no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when a restriction on processing has been lifted.

16. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied, or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

• To personal data that an individual has provided to us

• Where the processing is based on the individual's consent or for the performance of a contract

• When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. We will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual, but we are not required to adopt or maintain processing systems which are technically compatible with other organisations.

If the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

We will respond to any requests for portability within one month.

Where the request is complex, or several requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the Trust or Information Commissioner.

17. The right to object

We will inform individuals of their right to object and this is outlined in the privacy notice.

Individuals have the right to object to the following:

• Processing based on legitimate interests or the performance of a task in the public interest

• Direct marketing

• Processing for purposes of scientific or historical research and statistics

Where personal data is processed for the performance of a legal task or legitimate interests:

• An individual's grounds for objecting must relate to their particular situation

• We will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can

demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

• We will stop processing personal data for direct marketing purposes as soon as an objection is received

• We cannot refuse an individual's objection regarding data that is being processed for direct marketing Purposes Where personal data is processed for research purposes:

• The individual must have grounds relating to their situation in order to exercise their right to object Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of data.

18.Privacy by design and privacy impact assessments

We will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into processing activities. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow us to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to our reputation which might otherwise occur. A DPIA will be used

when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

• Systematic and extensive processing activities, such as profiling

• Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences We will ensure that all DPIAs include the following information:

• A description of the processing operations and the purposes

• An assessment of the necessity and proportionality of the processing in relation to the purpose

• An outline of the risks to individuals

• The measures implemented to address risk

Where a DPIA indicates high risk data processing, we will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

19. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff members will be made aware of, and understand, what constitutes as a data breach as part of their induction and ongoing training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner will be informed with all notifiable breaches reported within 72 hours of the Academy or Trust becoming aware of it.

If a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly as soon as reasonably possible after becoming aware of the data breach.

Effective and robust breach detection, investigation and internal reporting procedures are in place across the

Trust, which aid decision making in relation to who should be notified of a breach.

Within a breach notification, the following information will be outlined:

The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

The name and contact details of the academy based Data Protection Lead who in turn will report to the Data Protection Officer An explanation of the likely consequences of the personal data breach A description of the proposed measures to be taken to deal with the personal data breach

20. Data security

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. We will ensure that:

• The network security is effectively operating and updating

• Software updates are applied to minimise vulnerabilities

• Antivirus and Anti Malware is installed to prevent malware, which is intentionally designed to cause damage to the computer, server, client or computer network

• Access to systems will be minimised and be based on needs and requirement of users

• Secure configuration will be adopted when installing computers and network devise to reduce the risk of cyber threats

• Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and will not be left unattended or in clear view anywhere with general access

• Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network

drive that is regularly backed up off-site. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted

• All electronic devices are password-protected to protect the information on the device in case of theft

• Staff will not use their personal laptops, computers or mobile phones to store the data of students, parents/carers or other members of staff

• All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password

• Passwords will be at least 8 characters long and will contain letters, numbers and symbols. Staff will be reminded to change them at regular intervals

• Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient

• Circular emails to parents/carers are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients

• When sending confidential information by fax, staff will always check that the recipient is correct before sending

• Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from Trust premises accepts full responsibility for the security of the data

Before sharing data, all staff members will ensure:

• They are allowed to share it

• That adequate security is in place to protect it

• Who will receive the data has been outlined in a privacy notice

• They will check if unsure

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times.

The physical security of buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

CoBF takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer is responsible for continuity and recovery measures being in place to ensure the security of protected data.

21.Publication of information

We publish a publication scheme on our website outlining classes of information that will be made routinely available, including:

• Policies and procedures

• Annual reports

• Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

We will not publish any personal information, including photos, on our website without the permission of the relevant individual.

When uploading information to our websites, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

22.CCTV

We understand that recording images of identifiable individuals constitutes as processing personal information and so it is done in line with data protection principles. CCTV Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil a legitimate purpose such as for safety and security. Staff, students and visitors are notified of the purpose for collecting CCTV images via notice boards, letters and email.

All CCTV footage will be kept for 60 days for security purposes; the individual academies Data Protection Lead is responsible for keeping the records secure and allowing access.

We will always indicate our intentions for taking photographs or film of students or at Trust or academy events and will ensure we have permission before publishing them.

23.Photography

As part of our academy's activities, we may take photographs and record images of individuals within our academies.

The academy will obtain written consent from parents/carers/guardians/student for the general use categories of photos and videos.

The academy will obtain written consent from parents/carers/guardians/student for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer/guardian and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Marketing and promotional materials uses may include:

• Within the academy on notice boards and in academy magazines, brochures, prospectuses newsletters, etc.

• Children's books to evidence their learning

• Outside of the academy by external agencies such as the academy photographer, newspapers, campaigns

• Online on our academy website or social media pages

When using photographs and videos in this way the academy will not include any other personal information about the child, to ensure they cannot be identified, unless parent/carer/guardian/student consent is provided, and

safeguarding is not compromised. 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.

24. Data retention

CoBF has an agreed retention schedule in place which broadly follows the guidelines from the Annual Review of School Records and Safe Data Destruction IMRS (information and Management Records Society) checklist approved by the DFE.

Data will not be kept for longer than is necessary and will be deleted as soon as practicable. Information will be retained for at least the period specified in the retention schedule. Paper and Electronic records will be regularly monitored by the trust staff. The retention periods are based on business needs and legal requirements.

Some educational records relating to former students may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

25.Record Keeping

UK GDPR requires us to keep full and accurate records of all our data processing activities.

We keep and maintain accurate records reflecting our processing. These records include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

26. Training

All staff and governors 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 academy's processes make it necessary. Data Protection Leads will be provided with the training required to enable them to successfully undertake their roles.

27.Subject Access Requests

Individuals have the right to request access to information any organisation holds about them. This is known as a Subject Access Request (SAR).

Subject Access Requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing. The Trust has a Subject Access Form that we ask data subjects to complete. Requests can be made directly to the academies Data Protection Lead or to the trust Data Protection Officer. If a member of staff receives a Subject Access Request in any form, it must be immediately forwarded to either the DPL or the DPO.

The identity of the requestor will be established before the disclosure of any information, and if the request relates to a child's record checks will be carried out regarding proof of relationship to the child. The trust / academy will contact the individual to confirm they made a request. The trust/academy will require two forms of identity.

Any individual has the right of access to information held about them. However, with children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Principal / DPL will discuss the request with the student and take their views into account when making a decision. A student competent to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

If the individual (data subject) wishes to appoint a third-party representative, they must complete the

Authority of a Third-Party Representative SAR Form and provide identity documents for both themselves and their representatives. This form will be provided by the DPL / DPO upon request.

A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

All requests will be responded to without delay and at the latest, within one month of receiving it.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, we retain the right to refuse to respond to the request.

The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the Information Commissioner.

The UK GDPR and Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure. For example, we will not reveal information in response to subject access requests that:

• Might cause serious harm to the physical or mental health of the individual or another individual

• Would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests

• Includes information contained in adoption and parental order records

• Includes certain information given to a court in proceedings concerning the child

Where a request is received from an outside statutory organisation where there may be a safeguarding concern it must be noted that the DPA and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the Designated Safeguarding Lead.

Information can be provided at the academy with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should also be considered when considering the method of delivery. If postal systems have to be used, then registered/recorded mail will be used.

28. Disposal of records

We recognise that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf We will always choose a qualified source for disposal of IT assets and collections.

29.Links to other policies

This policy is linked to the following policies:

Freedom of Information Policy and Publication Scheme

CCTV Policy

E-safety Policy

Acceptable Use of IT

Code of Conduct

Protection of Biometric Data Policy

Chid Protection Policy

Records and Retention Policy

30.Complaints

Complaints about the above procedures should be made to the Data Protection Officer (DPO) who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's Complaints Procedure.

Complaints which are not appropriate to be dealt with through the Trust's complaint procedure can be dealt with by the Information Commissioner. Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

31.Contacts

If you have any queries or concerns regarding this policies advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk.