Codsall Multi-Academy Trust

Data Protection Policy

Growing as One

Commitment

Compassion

Community

Introduction

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Codsall Multi Academy Trust will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties. This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Section 1 – Definitions

Personal Data

Personal data is defined by the General Data Protection regulation (EU Regulation 2016/679((the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly in particular by reference to an identifier'. These can include:

• Names of individuals.

• Postal addresses.

• Email addresses.

• Telephone numbers.

• Any other information relating to individuals.

Special Category Data Previously termed "Sensitive Personal Data",

Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

The organisation storing and controlling such information (i.e. the Trust) is referred to as the Data Controller. Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them. DPIAs are designed to help organisations to systematically analyse, identify and minimise the data protection risks of a project or plan. These form a key part of our accountability obligations under UK GDPR.

Section 2 – When can the trust process personal data

Data Protection Principles

The Trust are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR. The principles the Trust must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner The Trust only collect, process and share personal data fairly and lawfully and for specified purposes. The Trust must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

• The data subject has given their consent;

• The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;

• To protect the data subject's vital interests;

• To meet our legal compliance obligations (other than a contractual obligation);

• To perform a task in the public interest or in order to carry out official functions as authorised by law;

• For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation.

This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

• The data subject has given their explicit consent;

• The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;

• To protect the data subject's vital interests;

• To meet our legal compliance obligations (other than a contractual obligation); • Where the data has been made public by the data subject;

• To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;

• Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

• Where it is necessary for reasons of public interest in the area of public health;

• The processing in necessary for archiving, statistical or research purposes. The Trust identifies and documents the legal grounds being relied upon for each processing activity. Consent Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them.

Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required). A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. If explicit consent is required, the Trust will normally seek another legal basis to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent. The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes. The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes. When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. Please refer to the Trust's Data Retention Policy for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data. Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data. We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices. Please refer to the Trust's Retention Policy for further details about how the Trust retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage In order to assure the protection of all data being

processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

• Encryption;

• Multi-Factor Authentication

• Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);

• Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);

• Adhering to confidentiality principles;

• Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data. The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data

The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

• Has a need to know the information for the purposes of providing the contracted services;

• Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;

• The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

• The transfer complies with any applicable cross border transfer restrictions; and

• A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our Trust shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance

with the GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Section 3 – Data subject's rights and requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data. The rights data subjects have in relation to how the Trust handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the Trust's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);
(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

Direct Marketing

The Trust are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls). The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must: -

• Only access the personal data that you have authority to access, and only for authorised purposes;

• Only allow others to access personal data if they have appropriate authorisation;

• Keep personal data secure (for example by complying with rules on access to Trust premises, computer access, password protection and secure file storage and destruction);

• Not to remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

• Not to store personal information on local drives.

Section 4 – Accountability

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles. The Trust have taken the following steps to ensure and document GDPR compliance: - Data Protection Officer (DPO)

Please find below details of the Trust's Data Protection Officer:

- Data Protection Officer: Entrust: Natalie Morrissey dpo.schools@staffordshire.gov.uk

The Trust is responsible for overseeing this data protection policy and developing data-related policies and guidelines. Please contact the CFOO with any questions about the operation of this Data Protection Policy or the DPO or if you have any concerns that this policy is not being or has not been followed.

In particular, you must always contact the in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the Trust to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;
(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Point of Contact

Each academy has a lead contact for GDPR, when reporting suspected breaches please use the contact table below, if a breach or suspected breach is discovered outside of term time then these must be reported to the academy lead and the trust leads immediately.

CMAT Central Team	Birches First School	St Nicholas CE First School	Codsall Middle School
cfoo@cmat.academy CFOO : Ian Moore	office@birches.staffs.sch.uk	office@st-nicholas.staffs.sch.uk	office@codsall-middle.staffs.sch.uk
ceo@cmat.academy CEO : Jodie Parker	headteacher@birches.staffs.sch.uk Head Teacher : Sabrina Varricchione.	headteacher@st-nicholas.staffs.sch.uk Head Teacher: Jodie Parker	headteacher@codsall-middle.staffs.sch.uk Head Teacher Kirstin Reade

Personal Data Breaches

The GDPR requires the Trust to notify any applicable personal data breach to the Information Commissioner's Office (ICO). We will put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches at the academy or at the trust, these contacts can be found on the point of contact section within this policy.

Personal Data Breach Reporting Procedure

This procedure is based on guidance regarding 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 academy/trust lead and the academy Principal.

• The academy/trust lead will report the incident to the DPO.

• The academy and/or central trust team will investigate and appoint a leading officer to report back to the DPO to determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidently 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 ICT Business Partner, Directory of Operations and Principal/Academy Business Manager where appropriate.

• The trust and/or academy 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 is reportable 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 dame (e.g. emotional distress), including through:

• Loss of control over their data

• Discrimination

• Identity theft or fraud

• Financial loss

• Damage by 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.

• Where the ICO must be notified, the DPO will do this via the 'report a breach' section of the ICO website within 72 hours of the breach.

As required, the DPO will set out:

• A description of the nature of the personal data breach including, where possible:

o The categories and approximate number of individuals concerned.

o The categories and approximate number of personal data records concerned. • The name and contact details of the leading officer.

• 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 together with the academy and or the trust 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 academy and/or trust will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

o The name and contact details of trust/academy and the leading officer appointed. o A description of the likely consequences of the personal data breach .

o 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 academy and/or trust 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:

o Facts and cause

o Effects

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

• The DPO, ICT Provider, CFOO, and where appropriate the academy HeadTeacher and C.E.O. will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible after the DPO has reached their conclusion to the breach.

Transparency and Privacy Notices

The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the Trust use their data and the Trust's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice. When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The

Trust will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR.

Privacy By Design

The Trust adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner. Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Trust conduct DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event the Trust carries out DPIAs when required by the GDPR in the following circumstances: -

• For the use of new technologies (programs, systems or processes) or changing technologies;

• For the use of automated processing; • For large scale processing of special category data;

• For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV). Our DPIAs contain: -

• A description of the processing, its purposes and any legitimate interests used;

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

• An assessment of the risk to individuals; and

• The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The Trust are required to keep full and accurate records of our data processing activities. These records include: -

• The name and contact details of the Trust;

• The name and contact details of the Data Protection Officer;

• Descriptions of the types of personal data used;

• Description of the data subjects;

• Details of the Trust's processing activities and purposes;

• Details of any third-party recipients of the personal data;

• Where personal data is stored;

• Retention periods; and

• Security measures in place.

Training

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The Trust through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

Related Policies

Staff should refer to the following policies that are related to this data protection policy:

Records Management Policy

Privacy Policy

These policies are also designed to protect personal data and can be found on the Trust website Monitoring We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

Appendix 1 – Subject Access Requests Under Data Protection Law,

Data Subjects have a general right to find out whether the Trust 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 Trust are undertaking. A Data Subject has the right to be informed by the Trust 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 Trust'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 child):

• for confirmation as to whether the Trust 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 Trust hold 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 Trust 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 which 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 the CFOO and/or ICT Business Partner – email –cfoo@cmat.academy who should contact Entrust as DPO in order to assist with the request and what is required.

Acknowledging the request

When receiving a SAR the Trust shall 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 Trust 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 Trust must clarify what address/email address to use when sending the requested information; and/or

• consent (if requesting third party data). The Trust 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 Trust 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 Trust 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 Trust 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 Trust 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 Trust 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 Trust do not receive this information, they will be unable to comply with the request. Requests made by third parties or on behalf of children The Trust need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement.

This might be a written authority to make the request or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances. When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data.

Before responding to a SAR for information held about a child, the Trust should consider whether the child is mature enough to understand their rights. If the Trust is confident that the child can understand their rights, then the Trust should usually respond directly to the child or seek their consent before releasing their information. It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

When considering borderline cases, it should be taken into account, among other things:

• the child's level of maturity and their ability to make decisions like this;

• the nature of the personal data;

• any court orders relating to parental access or responsibility that may apply;

• any duty of confidence owed to the child or young person;

• any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment; • any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

• any views the child or young person has on whether their parents should have access to information about them.

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

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child. Fee for responding to a SAR The Trust 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 Trust 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 Trust 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. Page 17 of 18 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 Trust are 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 Trust have one month in which to respond the Trust 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 Trust 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 Trust is not allowed to amend or delete data to avoid supplying the data. How to locate information

The personal data the Trust need 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.

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 Trust 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 Trust 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 Trust disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the Trust 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 Trust 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 caseby-case basis after a careful consideration of all the facts.

Crime detection and prevention: The Trust do 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 Trust do 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 Trust receive 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 Trust must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The Trust do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The Trust do 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 Trust do 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.