



Data Protection Policy

Primary and Secondary Academies

May 2018

1. Introduction and scope

- 1.1 CHAT Academies have a legal responsibility to ensure it and all academies comply with the requirements of the General Data Protection Regulations. This is the law which protects personal privacy and applies to any school or academy which processes or has access to people's personal data.
- 1.2 The legislation helps ensure that the management of data held electronically and / or and in paper-based systems are processed correctly and also gives rights to the people about who the data relates. CHAT Academies are named as the '*Data Controller*' i.e. the personal data owner responsible for ensuring workplace practices and policies are in place
- 1.3 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary

2. Definitions

2.1 **Personal data**

Data which can identify a living individual. This includes data that when combined with other readily available information, can lead to a living individual being identified. It also applies to data held visually in photographs or video clips (including CCTV) or as audio recordings.

2.2 **Special categories of personal data**

Such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical / mental health (or condition), sex life, sexual orientation, and biometric data.

2.3 **Processing**

The obtaining, recording or holding of personal data

2.4 **Data subject**

The person(s) whose personal data is held or processed

2.5 **Data controller**

The owner of the data who determines the purposes for and the manner in which personal data is processed other than that which they are required to by law

2.6 **Data processor**

A person / organisation who processes personal data on behalf of the data controller (This does not include employees of the data controller)

3. Data protection principles

- 3.1 We are obligated to document the personal data we are processing and how long / why we are holding it. We are also obligated to follow the principles set out in the Data Protection Regulations which state that all personal information, or data, about individuals should be: -

a) **Processed fairly and lawfully**

In the absence of an overriding necessity or legal requirement to do so, consent is required to process personal data. In any event, individuals should be made fully aware of why we are

collecting their information, what we intend using it for, and who else we may be sharing it with. Our [Privacy Notice](#) is available on our website.

b) Collected for specified, explicit and legitimate purposes

We will only process the personal data we've collected for the purposes we said we would when it was collected.

c) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

We will only collect and process the information we need as opposed to any additional information that may be useful in the future for another purpose.

d) Accurate and, where necessary, kept up to date

We will regularly review the information we hold to ensure that personal data is kept up to date.

e) Kept no longer than is necessary for the purpose for which it is processed

Depending on the overriding need of any legislation, statutory or legal requirement, data will not be kept longer than is required for the purposes of processing.

f) Processed in a way that ensures it is appropriately secure

We are obliged to ensure that personal data is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

3.2 Personal information cannot usually be released to anyone else without the data subject's consent or knowledge. However, there are certain circumstances when a third party (such as a government agency or law enforcement agency) can request information and we may be obliged to provide it to them (for example where the disclosure is required by law or by a court order).

3.3 We do however have a statutory obligation to report some statistical information to the DfE (for example the school and workforce census). More information about where share personal data can be found in our [Privacy Notice](#) available on our website

4. The right to be informed

4.1 Whenever we collect personal data we must make it clear to the data subject: -

- who we are
- the contact details of our Data Protection Officer if should there be any queries
- what we are collecting
- why we are collecting it and if there is a statutory requirement for us doing so
- where it will be held
- how long we will hold it
- where it will be shared (especially if internationally)

- whether we use it in any way to analyse or predict behaviour (and whether those predictions are performed automatically)
- what may happen if you we're not provided with the data we seek;
- of their right to withdraw consent (unless we have a statutory duty to process it of course);
- of their right to complain to the data protection regulator (www.ico.org.uk); and
- of any additional rights they have (which are further clarified later in this guidance)

4.2 The above is fully explained in our **Privacy Notice** available on our website. **Data Protection Officer contact details can be found at the end of this document in APPENDIX 1**

5. Requesting personal data (the right of access)

5.1 Individuals have a right to request access to personal data which the Trust holds about them. This is known as a 'subject access request'

5.2 A person to whom the personal data relates is about is known as the '*data subject*' and the person who is making the request is known as the '*applicant*'.

A common example of this relationship would be when a parent (*applicant*) is seeking personal information about their child (*data subject*).

The applicant and the data subject can of course be the same person.

5.3 It should be noted that any personal data we hold other than for the purposes of delivering education actually belongs to the pupils. So, whilst someone with parental responsibility may make a request for personal data about their child, data protection legislation requires a data controller to assess the competency of a data subject and this is not simply restricted to their age. i.e. 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.

5.4 Parents do have rights outside of data protection with regard to educational information of their child whilst they are of statutory school age.

What we will require

5.5 Whilst we would prefer to receive a request in writing, a request for the personal data can be made in person by contacting the academy office or our Data Protection Officer directly. **Contact details can be found at the end of this document in APPENDIX 1**

5.6 Whichever way the request is made we will require: -

- The name of the data subject
- The name of the applicant and their relationship to the data subject (if it is a different person)
- Details and / or a description of the data requested.
- Proof of identification

Anyone who is in regular contact with the academy may wish to make an appointment to confirm identification in person however we still may require photographic identification (such as a valid passport or driving licence)

- Proof of postal address
if you wish us to securely post the information to you we will require proof of current address. Information can alternatively be disclosed in person once identification is confirmed
- A contact number / email address
We may need to contact you to seek clarification or additional details from you to help us locate the personal data if we are unsure where what you seek can be found.
It is unlikely we will disclose personal data via email unless it is a secure email address or a password encrypted attachment.

- 5.7 Anyone making a request on someone else's behalf must provide us with that person's signed, written consent, or proof that they are legally entitled to act on their behalf. We still may need to verify this as per Section 5.5 above
- 5.8 There should be no financial cost to you however if you are seeking additional copies of data we have already provided or the request itself is manifestly unfounded or excessive then there may be a reasonable administration fee applied.
- 5.9 Following receipt of the written request and confirmation of identity / address, the response will be disclosed within a calendar month
- 5.10 Depending on the nature of the request and the volume of data sought, the response timescale may be extended by two further calendar months and should this be case will be communicated to the applicant ahead of the original deadline.
- 5.11 If we do not have enough information required to perform a search we will contact the applicant and ask for more details.
- 5.12 It should be noted that it is an offence for a person to knowingly or recklessly obtain or disclose personal data without the consent of the controller, to procure the disclosure of personal data to another person without the consent of the controller, or (after obtaining personal data) to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

What you will receive

- 5.13 Unless there are any exemptions which may apply, the data subject can expect to receive a copy of the personal data they seek including (unless it is otherwise made clear in the data you receive) the following information: -
- Why we are processing the personal data
 - What we are processing
 - Which other organisations receive the personal data

- How long we hold the personal data
- An explanation of rights to erase, amend or restrict the processing of any personal data
- Their right to complain to the data protection regulator (The Information Commissioner)
- The source of any personal data we hold that we did not collect from the data subject directly
- Whether we use the data in any way to analyse or predict behaviour
- Whether there have been any incidents of us transferring any personal data to another country and how safely we have made this transfer

What are exemptions?

5.14 There may be occasions where we are unable to provide the personal data requested. Where this is the case and where we are able to do so, we will inform you of the reasons why any of the personal data sought has been withheld from you.

5.15 Some examples of when this situation may arise in an academy school setting are: -

- If the data sought belongs to another person (third party) who has not consented to us disclosing this information
- If the data sought was processed for the prevention / detection of crime and releasing it could prejudice an investigation. This is an example of where we may not even be able to inform you why it has not been released as the mere indication that this exemption was used may highlight that it was used in relation to the prevention / detection of crime and generate prejudice.
- If, after seeking professional advice, we genuinely believe that releasing the data sought could cause mental or physical upset to the applicant or data subject. This is another example of where we may not be able to inform you of the reasons for withholding this data
- There may be potential or ongoing legal proceedings which prevent us from disclosing the information

6. The right to data portability

6.1 Similar to and arguably part of 'subject access' in Section 5 above, this right allows individuals to request a copy of any data we have collected in a structured, commonly used and machine readable format.

6.2 A copy of the raw data we hold which may be useful if it is transferred to another organisation which uses a similar system and for the purposes of continuity of monitoring

7. The right to object

7.1 This broad term applies to specific situations and this right applies if the data subject feels we have neither an official authority nor a legitimate interest to process their personal data

7.2 As per our [Privacy Notice](#) available on our website, we are legally obliged to process some personal data

7.3 Whilst consent will always be sought and can be withdrawn at any time, individuals can object to us using personal data for direct marketing and research purposes. We may not be obliged to stop processing the personal data for research purposes if it is being archived in the public interest.

8. The right to rectification

8.1 We have a duty to ensure personal data we hold is accurate and up to date however individuals should also inform us if / when personal data changes (e.g. a change of address or contact details)

8.2 There may be times when what we feel is accurate personal data does not match what individuals feel is accurate data. This right allows the data subject to request we correct the personal data we hold as soon as is practicable and without undue delay.

8.3 However, there may be situations where the data we hold cannot be amended as it may relate to something we genuinely felt was accurate at the time and that subsequent decisions were made because of it (e.g. the sanction of a detention may have occurred following a recorded behavioural incident which was latterly disputed). Supplementary statements may be added to further expand on the situation surrounding the event in question.

8.4 In both 8.2 and 8.3, we may have to cease processing the personal data whilst we resolve the matter but this will be further explained in 'the right to restrict processing' below (Section 10).

8.5 Should the result be that personal data needs to be amended, we will ensure that it is amended across the organisation and notify anyone else we may have disclosed the personal data to so that their records are also updated

9. The right to be forgotten (aka the right to erasure)

9.1 Individuals have the right to request that we remove all personal data we hold about them in certain circumstances. They can request we erase personal data where: -

- It is no longer necessary for us to process the personal data we hold (i.e. the purpose for processing has passed.)
- They inform us that they have withdrawn their consent for us to process any personal data which could only go ahead with consent (and there are no legal grounds for us to continue)
- They have objected to us processing personal data and this objection has been upheld. See 'the right to object' above (Section 7).
- They feel we are processing personal data unlawfully
- There is a law or legal obligation (such as a court order) which requires us to erase the personal data

9.2 We also recognise the future right of (those who will eventually become) former pupils to request that their image is removed from information society websites (such as social media) where their parent may have consented on their behalf when they were under 13 years of age

- 9.3 We therefore have a duty to ensure our new systems and technologies allow us to oblige a request to be forgotten and where older systems were in place before the new regulations came in to power, we will make all reasonable steps to ensure a request is complied with.
- 9.4 Should the result of a request be that personal data needs to be erased, we will ensure that it is erased across the organisation and notify anyone else we may have disclosed the personal data to so that they can also remove it from their records.
- 9.5 Please note however that there may be occasions where we are unable to erase personal data. This will usually be where it is necessary: -
- for compliance with a legal obligation which requires processing (such as our requirement to process and report on personal data with regards to the delivery of education)
 - if the personal data is being used to establish, exercise or defend against legal claims
 - where we may have a public interest in protecting public health
 - for exercising the right of freedom of expression and information
- 9.6 If the data is being archived in the public interest or for scientific / historical research we may also not be obliged to erase it if its removal would significantly affect the research. We would have always informed individuals that were going to do this and sought consent when the data was collected as per our [Privacy Notice](#) available on our website. We would also codify the personal data in such a way that individuals could not be identified. (This is known as 'Pseudonymisation'.)

10. The right to restrict processing

- 10.1 This right allows individuals to request we put the processing of their personal data 'on hold' whilst we are in the process of considering requests made under other rights outlined above.:
- 10.2 Examples in our academy schools where we can put processing 'on hold'
- Whilst the accuracy of personal data we hold is being questioned (see 'the right to rectification' above):
 - If someone feels that we are holding their personal data unlawfully they'd rather we held on to it as opposed to erasing it whilst they decide what they wish to do
 - If the personal data was scheduled to be destroyed but we are asked to hold on to it by the data subject as it is required to establish, exercise or defend legal claims
 - If we receive an objection to us processing personal data because the data subject feels we have neither an official authority nor a legitimate interest to do so then we will place the data processing 'on hold' whilst we determine whether a claim is upheld
- 10.3 Whilst the restrictions are in place we will ensure that the data processing is 'on hold' across the organisation and notify anyone else we may have disclosed the personal data to so that they can restrict it also.

11. Rights related to automated decision making and profiling

11.1 This right allows the data subject to not be subject to a decision made based solely on *automated* processing (including profiling) i.e. a decision taken with no human involvement that produces legal effects which might negatively affect them

What is profiling?

11.2 Profiling is when personal data is analysed to predict certain actions of an individual. It doesn't have to be automated.

For example, we review pupil attendance patterns in order to put preventative actions in place as per our attendance policy and as we are required to do by law.

11.3 What is automated decision making?

11.4 Automated decision making is when personal data is used to come to a conclusion or a decision made without human intervention.

For example, the threshold of a number of pupil absences could be reached which generates a both an automatic fine and an appointment for a parent to meet with the Education Welfare Officer.

11.5 Whilst CHAT Academies do not make decisions this way (and would inform data subjects via our [Privacy Notice](#) and when we collected the personal data if we did) we have a duty to explain what the 'rights related to automated decision making and profiling' are, that you could express a right to object and challenge the automatic decision that was made if we did.

12. Education Records

12.1 Parents have rights with regard to education information about their child, however The Education (Pupil Information) England Regulations (2005) do not apply to non-maintained schools such as Academies.

12.2 Instead, The Education (Independent School Standards) (England) Regulations 2010 make provision for Academies to generate and send parents annual written reports relating to progress and attainment in the main subject areas taught.

12.3 Parents of children wishing to access education information that is not routinely shared with them must therefore make a request under the subject access provisions of the Data Protection Act as per Section 5 above.

13. Data security and storage of records

13.1 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.

14. Personal data breaches

- 14.1 The Trust and its academies will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the Data Protection Officer will make all reasonable efforts to contain and minimise the impact of the breach (assisted by relevant staff members or data processors where necessary)
- 14.2 The potential consequences will be assessed, based on how serious they are, and how likely they are to happen and the Data Protection Officer DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. Considerations will include whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage
- 14.3 When appropriate, we will report the data breach to the Information Commissioner within 72 hours.

15. Disposal of records

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

Data protection officer and individual academy contact details



Data Protection Officer

Cuckoo Hall Academies Trust

c/o Harmony House, Cuckoo Hall Lane, Edmonton, London N9 8DR

020 8804 4126 (ext 181)

information.access@chat-edu.org.uk



Cuckoo Hall Lane, Edmonton, London N9 8DR | 020 8804 4126

cuckoo@chat-edu.org.uk



1-3 Pitfield Way, Enfield, Middlesex EN3 5BY | 020 8805 9811

eha@chat-edu.org.uk



Queensway, Ponders End, London EN3 4SA | 020 8443 9631

heron@chat-edu.org.uk



40 The Ride, Enfield, London EN3 7GB | 020 8344 9890

kingfisher@chat-edu.org.uk



51 Nightingale Road, Edmonton, London N9 8BF | 020 8433 0708

woodpecker@chat-edu.org.uk