CHADWELL HEATH ACADEMY

Data protection/GDPR Policy

CHADWELL HEATH ACADEMY (the School)

Data protection/GDPR Policy

You must read this policy because it gives important information about:

- the data protection principles with which the School must comply;
- what is meant by personal information and sensitive personal information;
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- individuals' rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to the School's data protection officer, Saiful Islam

Introduction

1.1 The School obtains, keeps and uses personal information about individuals including its governors, pupils, parents, family members, next of kin and staff

(including job applicants, current and former employees, temporary and agency workers, student teachers, contractors, interns, volunteers and apprentices) for a number of specific lawful purposes, as set out in the School's data protection privacy notices.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to individuals. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The School's data protection officer is responsible for informing and advising the School and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the School's policies and procedures. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer Saiful Islam (office@chadwellacademy.org.uk 020 8252 5151)

2 Scope

2.1 This policy applies to all processing by the School of the personal information of individuals.

2.2 Staff should refer to the School's data protection privacy notices and, where appropriate, to its other relevant policies including in relation to *internet, email and communications, monitoring, social media, information security, data retention, use of images of children, bring your own device (BYOD) and criminal record information*, which contain further information regarding the protection of personal information in those contexts.

2.3 We will review and update this policy periodically in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

3 Definitions

3.1.1 "**criminal records information**" means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

3.1.2 "**data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

3.1.3 "**personal information**" (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

3.1.4 "**processing personal information**" means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

3.1.5 "**pseudonymised**" means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

3.1.6 "**sensitive personal information**" (also known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 The School will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep personal information accurate and up to date, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time (if it has not already started), and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the individual has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the School is subject;

(d) that the processing is necessary for the protection of the vital interests of the individual or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; and/or

(f) that the processing is necessary for the purposes of legitimate interests of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual — see clause 5.2 below.

5.1.2 except where the processing is based on consent, 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);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices;

5.1.5 where sensitive personal information is processed, also identify a condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a condition for processing that information (see paragraph 7.2.2 below), and document it.

5.2 When determining whether the School's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision; (see Appendix 1 attached)

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 The School may from time to time need to process sensitive personal information.

6.2 We will only process sensitive personal information if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with the School's legal obligations or for the purposes of the School's legitimate interests; and

6.2.2 one of the conditions for processing sensitive personal information applies, e.g.:

(a) the individual has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the School or the individual;

(c) the processing is necessary to protect the individual's vital interests, and the individual is physically incapable of giving consent;

(d) processing relates to personal information which is manifestly made public by the individual;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 The School's data protection privacy notices set out the types of sensitive personal information that the School processes, what it is used for and the lawful basis for the processing.

6.4 Before processing any sensitive personal information of a type or for a purpose not referred to in the School's data protection privacy notice, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

6.5 Processing of sensitive personal information of a type or for a purpose not referred to in the School's privacy notices will not occur until:

6.5.1 the assessment referred to in paragraph 6.4 has taken place; and

6.5.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.6 The School will not carry out automated decision-making based on any individual's sensitive personal information.

6.7 In relation to sensitive personal information, the School's procedures to ensure compliance with the data protection principles set out in paragraph 4 above include the following set out in paragraphs 6.116.12 below.

Governors

6.8 We process sensitive personal information contained in passports only to obtain criminal records information and confirm identity.

Parents, family members and next of kin

6.9 We process contact details of parents, family members and next of kin (which may include sensitive personal information) only for the purpose of contacting those individuals.

Pupils

6.10 We process medical and health information about pupils only to protect their welfare and comply with our legal obligations. We process information relating to pupils' race or ethnicity only to comply with our legal obligations.

Staff

6.11 **During recruitment**: we do not (except where the law permits otherwise):

6.11.1 consider sensitive personal information e.g. relating to race or ethnic origin, trade union membership or health, during the short-listing, interview or decision-making stages;

6.11.2 if sensitive personal information is volunteered, no record is kept of it and any reference to it is immediately deleted or redacted;

6.11.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and will not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.11.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.11.5 we will only ask health questions once an offer of employment has been made.

6.12 **During employment**: we will process:

6.12.1 health information only for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.12.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. [Where possible, this information will be anonymised];

6.12.3 trade union membership information only for the purposes of staff administration and administering 'check off';

6.12.4 details of family relationships (only for the purposes of identification, contacting family members or providing benefits to them or staff) which may contain sensitive personal information.

6.13 Staff members are required to take particular care in relation to their processing of sensitive personal information.

6.14 All sensitive personal information must be retained and disposed of in accordance with the School's specified retention periods.

7 Criminal records information

7.1 We process criminal records information about governors, staff and volunteers to comply with our legal obligations.

7.2 We will only process criminal records information if:

7.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. to comply with the School's legal obligations, where it is necessary for performance of a public interest task, or for the purposes of the School's legitimate interests; and

7.2.2 one of the conditions for processing criminal records applies, e.g.:

(a) the individual has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the School or the individual;

(c) processing relates to personal information which are manifestly made public by the individual;

(d) the processing is necessary for the establishment, exercise or defence of legal claims; or

(e) the processing is necessary for reasons of substantial public interest.

7.3 The School's data protection privacy notices describe the School's processing of criminal records information, what it is used for and the lawful basis for the processing.

7.4 Before processing any criminal records information for a purpose not referred to in the School's data protection privacy notice, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

7.5 Processing of criminal records information for a purpose not referred to in the School's privacy notices will not occur until:

7.5.1 the assessment referred to in paragraph 7.3 has taken place; and

7.5.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7.6 The School will not carry out automated decision-making based on any individual's criminal records information.

7.7 Staff members are required to take particular care in relation to their processing of criminal records information.

7.8 All criminal records information must be retained and disposed of in accordance with the School's specified retention periods.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the School is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer in order to assess whether a DPIA is required.

8.3 During the course of any DPIA, we will seek the advice of the data protection officer and, where appropriate, the views of affected individuals.

9 Documentation and records

9.1 We will keep written records of processing activities to the extent required by data protection law, including:

9.1.1 the name and details of the School (and where applicable, of other controllers, the School's representative and data protection officer);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of individuals and categories of personal information;

9.1.4 categories of recipients of personal information;

9.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

9.1.6 where possible, specified retention periods;

9.1.7 where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy notices;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal information;

9.2.5 DPIAs;

9.2.6 records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis and condition for our processing;

9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

9.4.1 updating our information audits to find out what personal information the School holds;

9.4.2 distributing questionnaires and talking to staff across the School to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9.4.4 We document our processing activities in electronic form so we can add, remove and amend information easily.

10 Privacy notice

10.1 The School will issue privacy notices from time to time, informing individuals about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Individual rights

11.1 Individuals have the following rights in relation to their personal information:

11.1.1 to be informed about how, why and on what basis that information is processed — see the School's data protection privacy notices;

11.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;

11.1.3 to have personal information corrected if it is inaccurate or incomplete;

11.1.4 to have personal information erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the School no longer needs the personal information but the individual requires the information to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where they do not think it is accurate (and the School is verifying whether it is accurate), or where they have objected to the processing (and the School is considering whether its legitimate interests override the individual's interests).

11.2 Individuals wishing to exercise any of the rights in paragraphs 11.1.3 to 11.1.6 will be invited in the School's data protection privacy notices to contact the data protection officer. Any staff member who receives a request from an individual to exercise these rights must immediately refer it to the data protection officer.

12 Individual obligations

12.1 Individual staff members are responsible for helping the School keep their personal information up to date. They should let the HR department know if the information they have provided to the School changes, for example, if they move house or change details of the bank or building society account to which they are paid.

12.2 Some members will have access to the personal information of other individuals in the course of their employment or engagement. If so, the School expects them to help meet its data protection obligations to those individuals.

12.3 Staff members who have access to personal information must:

12.3.1 only access the personal information that they have authority to access, and only for authorised purposes;

12.3.2 only allow other staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not staff to access personal information with specific authority to do so [from the data protection officer;

12.3.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions communicated by the School);

12.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the School's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device;

12.3.6 not store personal information on local drives or on personal devices that are used for work purposes, and comply with the School's IT policy.

12.4 Staff members should contact the data protection officer if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal information without a lawful basis for its processing or, in the case of sensitive personal information or criminal records information, without one of the conditions referred to in paragraphs 6.2.2 or 7.2.2 respectively being met;

12.4.2 any data breach as set out in paragraph 15.1 below;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the School's premises without appropriate security measures being in place;

12.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

13 Information security

13.1 The School will use appropriate technical and organisational measures in accordance with its IT policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where the School uses external organisations to process personal information on its behalf (so that those organisations are processors as defined in applicable data protection laws), additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of the School;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-processors are only engaged with the prior consent of the School and under a written contract;

13.2.5 the organisation will assist the School in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist the School in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to the School as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the School with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the School immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is

altered, the relevant staff must seek approval of its terms by the data protection officer.

14 Storage and retention of personal information

14.1 Personal information and sensitive personal information and criminal records information) will be kept securely in accordance with the School's IT policy, and/or the retention and records policy.

14.2 Personal information (and sensitive personal information and criminal records information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should adhere to the School's specified retention periods, or the criteria used to determine them. Where there is any uncertainty, staff should consult the data protection officer.

14.3 Personal information (and sensitive personal information and criminal records information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams;

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 The School will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;

15.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 The School will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

OR

16.2 The School may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) on the basis [that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of [binding corporate rules OR standard data protection clauses OR of compliance with an approved code of conduct. For ad hoc overseas transfers such as school trips, we will ask for explicit consent.

17 Training

The School will ensure that staff members are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The School takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the School; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

Appendix 1

Legitimate interests assessment (LIA)

How we apply legitimate interests in practice

If we rely on legitimate interests to justify information processing, we will use the three-part test to assess whether it applies.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that our processing is lawful. A record of the LIA will help us to demonstrate compliance in line with accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

The process

please follow these steps and record the judgements that are made.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests are an appropriate basis. There's no fool proof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified. Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome. Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing. If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk. If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.

CHADWELL HEATH ACADEMY

I have read and understood the Data Protection (GDPR) policy and agree to abide by its terms.

Name …….

(Print in full)

Signed.....

Date ……..