HCAT
Data Protection & GDPR Policy 2020

Reviewed 29/09/20

HCAT DATA PROTECTION AND GDPR POLICY 2020

Our Commitment:

HCAT is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

- Consent - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Contractual - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- Legal Obligation - processing is necessary for compliance with a legal obligation to which the controller is subject;
- Vital Interests - processing is necessary to protect the vital interests of the data subject or of another natural person;
- Public Interest - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Legitimate Interests - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The members of staff responsible for data protection are mainly Maxine Pearce and Rebecca Paddock. However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through CPD sessions.

The requirements of this policy are mandatory for all staff employed by the Academy Trust and any third party contracted to provide services within the school.

Notification:

Our data processing activities is registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:

https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO. Such breaches in a school context may include, but are not limited to –

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an Academy laptop containing non-encrypted personal data about pupils

Introduction

All academies within HCAT, collect and use certain types of personal information about staff, pupils, parents and other individuals who come into contact with the academy in order provide education and associated functions. The academies may be required by law to collect and use certain types of information to comply with statutory obligations. This includes CCTV images which may be used to capture material for security and safety purposes.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 1998 ("the DPA") and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The eight data protection principles as laid down in the DPA are followed at all times:

(1) Data must be processed fairly and lawfully, and only where one of the conditions in Schedule 21 can be met. If sensitive personal data, a condition in Schedule 3 must also be met

(2) Personal data shall be obtained only for one or more specific and lawful purposes

(3) Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed

(4) Personal data shall be accurate and where necessary kept up to date

(5) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose

(6) Personal data shall be processed in accordance with the rights of data subjects under the DPA

(7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

(8) Personal data shall not be transferred to a country outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

HCAT are committed to maintaining those principles at all times. This means that each academy will:

(1) Inform parents as to the purpose of collecting any information from them, as and when they ask for it

(2) Be responsible for checking the quality and accuracy of the information, regularly review the records to ensure information is not held longer than is necessary

(3) Ensure that when information is authorised for disposal it is done appropriately

(4) Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on your computer system

(5) Share personal information with others only when it is necessary and legally appropriate to do so, ensuring that pupil names are replaced with unique pupil numbers in the records before the data is transferred

(6) Set out clear procedures for responding to requests for access to personal information known as subject access in the DPA.

Personal Data

'Personal data' is information that identifies an individual. A sub-set of personal data is known as 'sensitive personal data'. Sensitive personal data is information relating to race or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health, sexual life or the commission of any offence. Sensitive personal data is given special protection.

HCAT does not intend to seek or hold sensitive personal data about staff or pupils except where they have been notified of the information, or it comes to their attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the academy their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood needed for other purposes, e.g. pension entitlements, may be indicative of some aspects of sexual life).

The DPA applies to all computerised data and manual files if they come within the definition of a relevant filing system. Broadly speaking, this means that they are readily searchable and it is easy to locate personal data within them.

Use of Personal Data by HCAT

It is required under the DPA that the personal data held must only be used for specific purposes allowed by law. The personal data held by academies applies to staff and pupils. For pupils this includes contact details, assessment/examination results, attendance information, special educational needs and photographs and may hold information about characteristics such as ethnic group and any relevant medical information.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the academy as a whole is doing, together with any other uses normally associated with this provision in an independent school environment.

HCAT may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the academy, but only where consent has been provided to this.

In particular, HCAT may:

(a) transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy;

(b) make use of photographs of pupils in academy publications and on the academy website;

(c) disclose photographs and names of pupils to the media (or allow the media to take photographs of pupils) for promotional and congratulatory purposes where a pupil may be identified by name when the photograph is published e.g. where a pupil has won an award or has otherwise excelled;

(d) keep the pupil's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the academy to their previous school.

Photographs with names identifying pupils will not be published on the academy website without the express permission of the appropriate individual. If parents wish to limit or object to any use of personal data, the Principal / Headteacher / Head of School should be notified in writing. Parents who do not want their child's photograph or image to appear in any of the academy's promotional material, or be otherwise published, must also make sure their child knows this.

Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the DPA will not apply e.g. where a parent takes a photograph of their child and some friends taking part in the school sports day.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/data-protection-self-assessment/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Security of Personal Data

HCAT will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this Policy and their duties under the DPA. HCAT will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Exemptions that Allow Disclosure of Personal Data to Third Parties

There are a number of exemptions in the DPA that allow disclosure of personal data to third parties, and the processing of personal data by the academy and its employees, which would otherwise be prohibited under the DPA. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely:

(1) the data subjects have given their consent;

(2) for the prevention or detection of crime;

(3) for the assessment of any tax or duty;

(4) where it is necessary to exercise a right or obligation conferred or imposed by law upon HCAT (other than an obligation imposed by contract);

(5) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

(6) for the purpose of obtaining legal advice;

(7) for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress); and

(8) where it is necessary to disclose the information for a legitimate interest HCAT or the third party to whom the disclosure is made.

Disclosure of Personal Data to Third Parties

HCAT may receive requests from third parties (i.e. those other than the data subject, the academy, and employees of the academy) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the academy.

The following are the most usual reasons an academy may have for passing personal data to third parties:

(1) to give a confidential reference relating to a pupil;

(2) to publish the results of public examinations or other achievements of pupils of the academy;

(3) to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

(4) to provide information to another educational establishment to which a pupil is transferring;

(5) to provide information to the Examination Authority as part of the examinations process; and

(6) to provide the relevant Government Department concerned with information relating to their functions as a regulator.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them.

Any wish to limit or object to any use of personal data by third parties, except as stated above, should be notified to the Principal / Headteacher / Head of School of the relevant academy in writing, or to the relevant authority (the contact details for which can be supplied by the academy).

Where the academy receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

Confidentiality of pupil concerns

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the academy will

maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the academy believes disclosure will be in the best interests of the pupil or other pupils.

Dealing with a Subject Access Request

Anybody who makes a request to see their file or their child's file or other personal data held on them is making a request under the DPA. All information relating to the individual can be considered for disclosure. This could include information held in day books, diaries and electronic systems as well as emails.

Where a child or young person does not have sufficient understanding to make his or her own request, a person with parental responsibility can make a request on their behalf. The Principal / Headteacher / Head of School must, however, be satisfied that:

(1) the child or young person lacks sufficient understanding; and

(2) the request made on behalf of the child or young person is in their interests.

HCAT will only grant pupils' access to their personal data if, in the relevant academy's reasonable belief, the pupil understands the nature of the request. It is generally accepted that, by the age of 12, a child can be expected to have sufficient maturity to understand the nature of the request.

Any individual, including a child or young person with ownership of their own information rights may appoint another person to request access to their records. In such circumstances the academy must have written evidence that the individual has authorised the person to make the application and the Principal / Headteacher / Head of School must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

A person who has parental responsibility for a child who does not have sufficient understanding to make their own Subject Access Request, may make a request for that child's personal information. In such circumstances, HCAT needs to be satisfied that the individual making the request does have the necessary parental responsibility, and that the request is in the interests of the child.

Access to records will be refused in instances where an exemption in the DPA applies, for example, information sharing may place a child at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A request under the DPA must be made in writing to the Trust, which must be responded to within 40 calendar days. Following this request, HCAT on behalf of the academy, may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves. The Principal / Headteacher / Head of School will have responsibility for ensuring the child's welfare is appropriately considered in deciding whether to comply with a request from a pupil and will make use of exemptions under the Act as appropriate.

All files must be reviewed before any disclosure takes place. Access will not be granted before this review has taken place. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

If an individual discovers that information which HCAT holds in relation to them is inaccurate or out of date, they should write to the Principal / Headteacher / Head of School, setting out the

inaccuracy, and the accurate position. This information should be corrected where HCAT agrees that the previous information was inaccurate.

If HCAT disagrees that the information is inaccurate, it will discuss the matter with the individual, but the academy has the right to maintain the original information. If the individual is unhappy with this outcome they have the right to instigate the appropriate procedure.

Educational records

Academies are not required to provide educational records if a parent requests it, as the Education (pupil information) Regulations 2005, which places this obligation on maintained schools, does not apply to academies. An academy may choose to comply but parents no longer have a legal right to this information.

The Independent School Standards Regulations which applies to academies by virtue of their funding agreement, states that the standard about provision of information is met if the Academy Trust ensures that an annual written report of each registered pupil's progress and attainment in the main subject areas taught, is sent to the parents of that registered pupil.

Exemptions to Access by Data Subjects

Confidential references given, or to be given by the academy, are exempt from access. HCAT will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil, member of staff, or volunteer.

It should be noted that confidential references received from other parties may also be exempt from disclosure, under the common law of confidence. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

Examination scripts, i.e. information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

Examination marks do not fall within an exemption as such.

However, the 40 calendar day compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the academy received the request (if all the necessary conditions set out in paragraph 34 are fulfilled), or 40 calendar days from the announcement of the examination results, whichever is the earlier.

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is exempt from disclosure unless the privilege is waived.

Repeated Requests for Access to Records

Unless a reasonable period of time has lapsed between the compliance with one request and receipt of the next, the DPA allows for access to be refused when the applicant has made repeated requests for information already provided.

Charging

If a pupil or parent requests information which does not form part of the educational record, the maximum fee which can be charged is £10 and must not exceed the cost of supplying the information. This also applies to a staff member requesting to see their personnel or other relevant records.

Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school administrator.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

• Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

• If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

• If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

• USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

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

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

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

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections.

The school also uses Restore to dispose of sensitive data that is no longer required.

Further advice and information, including a full list of exempt information, is available from:

Information Commissioner's Office (ICO) - https://ico.org.uk

Telephone: 0303 123 1113 or 01625 545 745.

Freedom of information

From January 2011, Academies became subject to the Freedom of Information Act 2000.

This policy will be updated as necessary to reflect best practice or amendments made to the DPA

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Principal / Headteacher / Head of School and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted
- by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

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

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's secured computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of
- potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach
    - and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the Trust's secured computer system

The DPO, and Principal / Headteacher / Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Below is a list that is not intended to be exhaustive but lists actions we will take for different types of sensitive personal data processed by an academy. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other risks of potential data security breaches we have already minimized are shown below:

- Details of pupil premium interventions for named children being published on the school website-; (No pupil level data is ever uploaded to the website).
- Non-anonymised pupil exam results or staff pay information being shared with governors- (This cannot happen as only anonymized results/finance documents shown or discussed with Governors.
- An academy laptop containing non-encrypted sensitive personal data being stolen or hacked - (Sensitive data is not stored on laptops.)
- The school's cashless payment provider being hacked and parents' financial details stolen- (External risk which the system provider mitigates against by complying fully with GDPR and ICT security legislation.)
- The school's payroll provider being hacked and staffs' financial details stolen- (External risk which the system provider mitigates against by complying fully with GDPR and ICT security legislation.)