CANNOCK CHASE HIGH SCHOOL

ACHIEVEMENT FOR ALL

DATA PROTECTION & FREEDOM OF INFORMATION POLICY

Contents

1 Policy Statement and Principles

1.1 Policy Aims and Principles

Through day to day activities, Cannock Chase High School (CCHS) holds a variety of personal information about staff, students and their parents/guardians. In some instances information may be held about staff and students' family members, such as next of kin. We are aware of our data protection responsibilities for individuals that are the subject of data collection and retention by CCHS and we will ensure that all data is treated fairly and lawfully.

The principles behind this policy are:

- To ensure that personal data is kept secure and confidential – preventing information passing into the wrong hands and reducing the risks of fraud attacks;
- To ensure employee's understand the importance of information rights as well as their own responsibilities for delivering them;
- To save time, effort and money by having effective procedures in place.

All employees are required to report instances of non-compliance of data protection principles detailed in this policy. All staff will have access to this policy and will be aware of who to contact with regards any of the procedures detailed.

This policy is consistent with all other policies adopted by CCHS and is written in line with current legislation and guidance. Failure to comply with this policy will be addressed without delay and may ultimately result in disciplinary action.

1.2 Data Protection and Freedom of Information

The Data Protection Act (DPA) exists to protect people's right to privacy, whereas the Freedom of Information Act (FOIA) removes unnecessary secrecy. These two aims are not necessarily incompatible but there can be a tension between them, and applying them sometimes requires careful consideration.

Personal information requested by third parties is exempt from release under the FOIA where this release would breach the DPA. If a request is made for information that includes someone else's personal data, we will carefully balance the case for transparency and openness under the FOIA against the data subject's right to privacy under the DPA to decide whether the information can be released without breaching the data protection principles. The information may be issued by redacting/blanking out the relevant personal information. In some instances, we may consult with a third party if their interests could be affected by release of the information requested.

1.2.1 Freedom of Information

Cannock Chase High School is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

What is a request under FOI?

Any request for any information from CCHS is technically a request under the FOI, whether the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Headteacher.

All other requests should be sent in the first instance to the DPO inbox (dpo@cannockchase-high.staffs.sch.uk) where it will be allocated to the Headteacher, who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request (see below).

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

Time limit for compliance

Cannock Chase High School must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For an Academy when calculating the 20-working day deadline, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

Procedure for dealing with a request

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the DPO inbox where it will be allocated to the Headteacher. The Headteacher will then liaise with the Leadership Team, and then may re-allocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether CCHS "holds" the information requested. The school will hold the information if it exists in computer or paper format. Some requests will require the school to take information from different sources and manipulate it in some way. Where this would take minimal effort, the school is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor will be contacted by the Headteacher to explain that the information is not held in the manner requested and offered the opportunity to refine their request. For example, if a request required the school to add up totals in a spread sheet and release the total figures, this would be information "held" by CCHS. If CCHS would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by CCHS, depending on the time involved in extracting the information.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the subject access regime in the DPA;
- Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles;
- Section 41 – information that has been sent to CCHS (but not the school's own information) which is confidential;
- Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;
- Section 22 – information that CCHS intends to publish at a future date;
- Section 43 – information that would prejudice the commercial interests of CCHS and/or a third party;
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
- Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.

The sections mentioned previously are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

Responding to a request

When responding to a request where CCHS has withheld some or all the information, CCHS must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by the Data Protection Officer, or by writing to the ICO.

Contact

Any questions about this policy should be directed in the first instance to the Headteacher. The Headteacher will ensure a suitable response to the enquirer on behalf of CCHS's Data Protection Team.

1.3 Complaints

All complaints are dealt with under the **CCHS Complaints Policy**. Complaints should be made in writing and will follow the CCHS complaint procedures and set timescales. The handling of complaints may be delegated to an appropriate person. The outcome of the complaint will be communicated in writing.

If the response is not satisfactory after exhausting the complaints process, the complainant should contact the Information Commissioners Office (ICO). The ICO can make a decision to

investigate a claim against the academy and take action against anyone who has misused personal data.

The contact details for the ICO are:
Telephone: 0303 123 1113 Website: http://www.ico.org.uk/complaints

1.4 Monitoring and Review

This policy will be reviewed annually or in the following circumstances:
- Changes in legislation and/or government guidance;
- As a result of any other significant change or event;
- In the event that the policy is determined not to be effective.

Governors will receive an annual report detailing any data breaches, both suspected and confirmed, any serious breaches will be reported immediately.

Any urgent concerns regarding the policy should be raised to the Data Protection Officer in the first instance for them to determine whether a review of the policy is required in advance of the planned review date.

2 Processing Personal Data

The DPA requires every organisation who is processing personal information to register with the ICO as a data controller. The registered data controller is CCHS.

We will only process personal data where there are legitimate grounds for collecting and using the personal data. Data will not be used in ways that have unjustified or adverse effects on the individuals that the data concerns. We recognise that certain types of data are more sensitive by nature than others and a Privacy Impact Assessment (PIA) will be conducted to determine any risks associated with processing any data. Information will be:
- Used fairly and lawfully;
- Used for limited, specifically stated purposes;
- Used in a way that is adequate, relevant and not excessive;
- Accurate;
- Kept for no longer than is absolutely necessary;
- Handled according to people's data protection rights;
- Kept safe and secure;
- Not transferred outside the UK without adequate protection.

2.1 Data Gathering

All personal data relating to individuals gathered by CCHS, whether held on computer, in paper files or other electronic media (CCTV), are covered by the DPA. To process this data fairly, we will provide the data subject details about the data's intended use, and inform them if the data may be used for other purposes or disclosed to another party. Individuals will be informed of this unless the collection and use of the data is:
- Something that a reasonable person is likely to anticipate and would agree to if asked;

- Is necessary to carry out the function the individual requested;
- Will have no unforeseen consequences for the individual concerned.

Information will be collected in a fair and open manner, we will tell individuals how the information will be used and who will be allowed to see it. Privacy notices will be issued explaining the purpose of the data collection wherever necessary.

2.2 Data Checking

Reasonable steps will be taken to ensure the accuracy of personal data. In order to do this we will:

- Issue regular reminders to ensure that personal data held is up-to-date and accurate;
- Rectify any errors discovered and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data;
- Make sure that the data provided is done so by the person it concerns (or someone acting on their behalf) and that any challenges to the accuracy of the information are carefully considered.

2.3 Data Retention

All personal data will be stored in a secure and safe manner in particular:

- Manual data will be stored where it not accessible to anyone without a legitimate reason to access it;
- Particular attention will be paid to the need for security of sensitive personal data.

<u>Electronic Data</u>
All computers will have adequate protection software, such as anti-virus, anti-malware or anti-spyware, which will be kept up to date. All unused or older versions of such software will be removed from the devices.

The use of mobile devices such as laptops may require additional protection, this will be proportionate to the level of risk associated with a particular device. Due to their potable nature, the chances of them being lost or stolen is increased therefore the personal data stored on such devices will be limited or removed.

Lost or stolen devices must be reported to the Business Manager within 24 hours.

All electronic data will be backed up on a regular basis and the backup will be kept securely and access will be restricted to essential staff members.

All staff members have been issued with an email address and access to secure sites. Security for these is of high importance and staff will be required to set strong passwords and renew passwords on a regular basis.

Sending data from a personal email account should be avoided, however, there are certain situations where this may be acceptable with prior approval. This will be done on a limited basis. If there is the need to send group emails then the academy will avoid including others email addresses by using blind carbon copy (BCC) not carbon copy (CC).

2.4 Using Data

Personal data will not be used in any newsletters, websites or other media without the consent of the data subject. We may incorporate consent into the data gathering sheets, to avoid the need for frequent or similar requests for consent being made.

Publication of Exam Results

The DPA does not stop the publishing of examination results. Publication can be done in a variety of ways, including posting lists of results on publicly accessible noticeboards, or providing examination results to the media.

We will act fairly in our decision to publish exam results and inform those involved whether results will be made public and how this will be done. This will be done as early as possible, at the start of the academic year and during each examination term.

Any concerns raised will be taken seriously and we will consider any objections before deciding to publish results and will provide the reason if a person's objection is rejected.

2.5 Sharing Data

Before sharing any personal data, we will consider all the legal implications of doing so and undertake a PIA to consider the potential benefits and risks of sharing data. We will always inform individuals of our intention to share data (if this has not previously been communicated and will gain consent where it is required).

When sharing data, we will put in place a data sharing agreement and ensure that the information is passed on in a secure way. Only the minimum information will be shared for the purpose of the agreement to meet the objectives, in all instances where the objectives can be met by anonymising data this will be done. A record will be kept of all data sharing agreements and will regularly review the agreements to ensure that data is not being shared unnecessarily.

Sharing Without the Individual's Knowledge

There may be instances where information is released to external bodies under one of the exemptions listed in the DPA. In particular this covers disclosing information for the prevention or detection of crime.

2.6 Archiving and Deleting Data

Personal data shall not be kept for longer than is necessary for the purpose it is collected. Data will be updated or archived if it goes out of date. If the data is no longer needed then it will be securely destroyed or deleted in line with the academy's retention and deletion schedule. All paper waste will be shredded and electronic copies will be permanently removed from computers/hard drives.

Data will only be archived instead of deleted if the information still needs to be retained. If data is deleted from a live system then we will ensure that any form of back up or copy will also be deleted. All personal information is removed prior to the disposal or old computers.

We will regularly review the data we hold and the length of time data is retained in accordance with regulatory and professional guidelines and our data and retention schedule. We will conduct a regular audit, involving checking through records to make sure data is not retained for too long and to ensure that data is not being deleted prematurely.

2.7 Dealing with a Breach of the DPA

In the event of a data security breach, Iain Turnbull, Headteacher, be informed immediately. If we become aware of a data breach we will:

- Investigate and contain the situation to limit the damage;
- Assess the risks associated with the breach;
- Identify potential adverse consequences for individuals;
- Inform the appropriate people and organisations that the breach has occurred;
- Accurately record the details of the breach and the actions taken;
- Where appropriate, inform the ICO and / or other third parties (police, insurers, professional bodies).

Following a breach of personal data we will evaluate the cause of the breach and the action taken to prevent similar breaches occurring in the future.

3 Protection of Biometric Information

Cannock Chase High School follows the advice set out in the Department for Education's document "Protection of biometric information of children in schools and colleges" which was is available by following this link: https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

4 CCTV

CCTV is used on academy premises to promote the safety and welfare of all individuals accessing the facilities. Images of people are covered by the DPA, this includes the information that can be derived from images. The CCTV system will only capture images of individuals and will not be used for audio recording.

The use of CCTV will be reviewed annually to ensure that it is effective.

All reasonable steps will be taken to ensure that individuals are aware that CCTV is in operation in specific areas.

The system used will have the necessary technical specification to ensure that images are of the appropriate quality and are not obstructed in any way. Cameras have been sited so that they provide clear images and so that they avoid capturing the images of individuals that is does not intend to capture. Regular checks will be carried out to ensure that the system is working properly and produces high quality images, this will include a check that the date and time stamp recorded on the images is accurate.

Images from the CCTV system are securely stored and only a limited number of authorised personnel may have access to them. The viewing of live images on monitors will be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.

The images will, in most instances, not be provided to any third parties with the exception of law enforcement bodies.

Requests for copies of an individual's own images will be dealt with as a Subject Access Request as detailed in Section 4 of this policy. We have discretion to refuse any request for information unless there is an overriding legal obligation to do so.

If images are disclosed then the method of disclosing them will be secure, ensuring that they are only seen by the intended recipient.

Once there is no reason to retain the recorded images, they will be deleted. The recorded images will only be retained long enough for:

- Any incident to come to light;
- And the incident to be investigated.

If at any point the use of CCTV processing requires working with another organisation, the academy will have a written contract with the processor which specifies exactly how the information is to be used and gives security guarantees.

4.1 Monitoring Staff

The use of CCTV is not intended to be used to monitor staff, however, they may be used if an incident arises that involves a member of staff or if something is seen on the footage that we cannot be expected to ignore, such as criminal activity, gross misconduct, or behaviour which puts others at risk.

If images are used in disciplinary proceedings, the footage will be retained so that the member of staff can see it and respond.

5 Subject Access Requests (SAR)

The DPA gives individuals the right to find out what information CCHS stores about them. This is known as a SAR.

If a data subject would like a copy of the information that is held about them then they must put this request in writing. The request can be sent by post, fax and email or via our social media sites, however, the preferred means of contact for such a request is either by post or email the data request to CCHS. Informal requests (oral) will be dealt with wherever possible.

As the data controller, CCHS is responsible for compliance with the DPA and an individual's right to make a SAR. If a request is made that relates to data that is held centrally (by CCHS) then CCHS will respond directly to this.

We will make reasonable adjustments for individuals with disabilities who choose to make a SAR. This will be done in accordance with the Equality Act 2010 and CCHS's **Equality Policy**.

We will make reasonable and proportionate efforts to find and retrieve the requested data in order to respond effectively to all SAR's. Information will be provided to the data subject in a permanent form unless the individual agrees otherwise, or doing so would be impossible or involve disproportionate effort.

Repeated, identical or similar SAR's made by the same person will not be responded to unless a reasonable interval has elapsed between the first request and any subsequent ones – if this occurs, we will inform the individual why the information has not been provided again.

5.1 Requests for Information about Children

We understand that personal data about a child belongs to the child and not their parent or guardian. If a SAR is made on behalf of a child then we will first consider whether the child understands their rights. If we are confident that they do then we will send the response of the SAR directly to the child the request is about.

If we do not believe that the child understands their rights in regards to a SAR then we will also take into account the following factors before releasing the information to the child or person with parental responsibility:

- 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 information or any detriment to the child if the information is not disclosed;
- Any views the child has on whether the information about them should be provided.

5.2 When Information can be Withheld

There is a legal requirement to provide a data subject with a copy of the information that is held about them if it is requested. However, there are some instances where information can be withheld. The DPA provides a number of exemptions.

The decision about whether to rely upon an exemption and withhold data is determined by CCHS and may be in relation to all of the information requested or just part of it.

If information is withheld in reliance on an exemption, we will respond promptly explaining, to the extent we can do so, the fact that information has been withheld and the reasons why. If only part of the information is withheld then as much information as possible will be disclosed.

Examples of information which the academy may consider be appropriate to withhold include:

- Information that might cause serious harm to the physical or mental health of the student or another individual;
- Information that would reveal that the child is at risk of abuse;
- Information contained in adoption and parental order records;
- Certain information given to a court in proceedings concerning the child.

If providing the information to an individual will disclose information about another person then we will only disclose this if we have received consent from the third party or it is considered reasonable in all the circumstances to comply with the request without consent. Information may be redacted that can identify another individual and where providing images from the CCTV system, images of third parties on the footage may be obscured or blurred.

5.3 Charges for SARs

A charge may apply for making a SAR. We will inform an individual of any charge we choose to apply without delay upon the receipt of the SAR. The following charges (exempt from VAT) may apply:

- £10 for the majority of SARs;
- £10 per disk for copies of CCTV footage;
- Up to £50 (dependent on the number of pages as detailed by the ICO) where a SAR is made for information containing, in whole or in part, a student's educational record.

5.4 Time Limits

The time limit for responding to most SARs is 40 calendar days. If the request is for a student's educational file then the time limit is 15 academy days.

The time limit begins once the request has been received providing that:

- Any fee applicable is paid;
- There are no doubts as to the identity of the data subject;
- The information requested is able to be located and identified from the SAR.

If we need to request payment and/or additional information the time limit will not begin until the data subject has provided payment and/or the information required.

If the request is made by a third party on someone else's behalf then they may need to provide evidence that they are entitled to do this, such as a power of attorney or letter of authority from the data subject. We will only request evidence or additional information if this is appropriate and considered necessary to ascertaining an individual's identity or to help us locate or identify the information.