The Polesworth School
ENSURING EXCELLENCE

Title of Policy: Data Protection Policy

Subtext (if applicable): relating to the Data Protection Act 1998, including readiness statement relating to the GDPR (General Data Protection Regulation) effective 25th May 2018

Member of leadership team with lead responsibility for oversight and update of policy	DIL
Approved at SLT	September 2017
Approved at Governing Body	November 2017
Policy review cycle	Normally bi-annually
Policy review date	In this instance by 28th May 2018

COMMUNITY ACADEMIES TRUST

DATA PROTECTION POLICY

This policy should be read in conjunction with the Data Protection Act 1998 (DPA), the Education Pupil (Information) Regulations 2005, Independent School Standards Regulations 2010 (applicable to academies), Privacy and Electronic Communication (EU Directive) Regulations 2003 and the ICO 'Report on the data protection guidance to schools'. In addition the ICO has produced guidance on readiness for the implementation of the GDPR (General Data Protection Regulation) which becomes effective on 25th May 2018. The school will keep this policy under review in the light of the UK Government's decision to move towards Brexit, at which time requirements under the Act may change.

Overview

For the purposes of the Act, the organisation registered with the ICO as Data Controller is Community Academies Trust. The Polesworth School is noted as a trading name of Community Academies Trust.

The Trust, schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- Have permission to access that data, and/or
- Need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the ICO – for the school and individuals involved. Particularly, all transfer of data is subject of risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in the relevant legislation.

Introduction

At our school, we acknowledge that to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with the school. We are also obliged to collect and use data to fulfil our obligations to the Local Authority, Department for Education and other bodies. We deal with information properly in whatever way it is collected, recorded and used – on paper, electronically or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as sensitive personal data and we are aware of the extra care this kind of information requires. We ensure that our organisation treats all personal information lawfully and correctly. To this end, we fully endorse and adhere to the data protection principles as contained in the Data Protection Act 1998.

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Data protection principles

All members of staff employed in our school are required to adhere to the eight enforceable data protection principles as set out in the Data Protection Act 1998.

- Data shall be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up-to-date.
- Personal data shall not be kept for longer than is necessary for that purpose or those purposes. A process exists to archive "old data" within the SIMS database and other confidential electronic files. Paper files are reviewed at the end of each academic year and archived accordingly, with information retention complying with statutory guidelines.
- Personal data shall be processed in accordance with the rights of data subjects under the DPA.
- 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.
- Personal data shall not be transferred to a country or territory 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.

Information about the school's definition of "personal data" appears at appendix 3.

School practice

Within school we will apply the following criteria and controls. These are to:

- Notify the ICO that we process personal data and re-notify if procedures change or are amended.
- Observe fully the conditions regarding the fair collection and use of information. To achieve this we have in place and use a privacy notice – this is sent to parents at the beginning of the academic year.
- Meet our legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of the persons about whom information is held can be fully exercised under the Act. These include the right to be informed that processing is being undertaken, the right to access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal information. We will review the physical security of buildings and storage systems as well as access to them. All portable electronic devices must be kept as securely as possible on and off school premises.
- The school requires staff not to transfer personal information from secure school systems to any other system using personal email accounts, unencrypted memory sticks or personal hard drives.

- The school advises staff to ensure that laptops and computers are locked when not in use or are unattended, to ensure that access to confidential information cannot be made by parties other than the user of the device.
- Ensure that all Disclosure & Barring Service records (recruitment and vetting checks) are kept in a safe central place and that no unnecessary certification information is kept longer than six months.
- Ensure that personal information in not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information – see appendix 1.
- Have in place secure methods for safely disposing of all electronic and paper records.
- Be sure that photographs of pupils are not included in any school publication or on the school website without specific consent.
- Take care that CCTV that captures or processes images of identifiable individuals is done in line with the data protection principles.
- Up to date virus and malware checking software is used to protect the school network from intrusion, ensuring that the data we hold is adequately protected.
- The school is reviewing how it transfers data to other user groups (for example Governors) to ensure that data transfer ensures that data is suitably protected.

We shall also ensure that:

- There is a named person with specific responsibility for data protection within the school and that person will be the School Business Manager.
- All persons managing and handling personal information understand that they are responsible for following good data protection practice. Training will be given as part of the induction process for new staff and regular reminders will be given to staff about their responsibilities on at least an annual basis.
- All persons managing and handling personal information are advised of their responsibilities.
- Anyone wanting to make enquiries about handling personal information knows what to do.
- Anyone managing and handling personal information is appropriately supervised.
- Queries about handling personal information are properly and courteously dealt with.
- The way personal information is held, managed and used will be reviewed as appropriate.
- A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.
- When information is authorised for disposal, it is done appropriately.
- A protocol exists for the access arrangements for staff to the main school database for staff & students (SIMS). As part of this protocol, a framework has been agreed that is a hierarchy of access rights, so that staff only have access to information and staff and students that they need to have in order to fulfil their professional responsibilities. Access rights are subject to a review cycle that is no longer than one academic year.

Secure storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole information management system.

All users will have strong passwords which must be changed regularly. User passwords must never be shared. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left unattended and set

to auto-lock if not used for 4 minutes. Personal data can only be stored on school equipment. Private equipment must not be used for the storage of personal data.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required and suitably archive data in accordance with guidance.

Audit, logging and incident handling

Any incidents of accidental or deliberate data security breaches, including loss of protected data or breaches of an acceptable use policy will be dealt with by:

- Appointing a responsible person for each incident;
- An investigation taking place;
- An action plan for rapid resolution; and
- A plan of action of non-recurrence and further awareness training.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. Staff, parents and students need to be aware of the risks associated with publishing digital images on the internet, with the potential for avenues for such things as cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

Photographic consent

The school seeks consent for use of photographic images from parents of students before doing so.

Use of biometric information

The Protection of Freedoms Act 2012 includes measures which affects the school in respect of biometric recognition systems (i.e. fingerprint identification). For all pupils under 18, written consent of a parent is obtained before biometric data is collected.

Monitoring of computer systems

The school conducts passive monitoring of all computer systems to ensure that students and staff are protected and remain safe. Only where relevant and necessary will the school interrogate or investigate this information, in circumstances which might place a student, member of staff or the school at risk.

Online

The school has a separate policy relating to Online.

Social networking (relating to school)

The school has a separate policy relating to Social Networking, which details the steps the school takes under the duty of care to provide a safe learning environment for students and staff.

Communication protocol

The school has protocols relating to communication between staff colleagues, with students and with parents/carers.

Freedom of Information Act

The school has a separate policy relating to FOI.

CCTV

The school has a separate policy relating to CCTV.

Use of cookies – school website

The school displays a "cookies" notice on the school website to users.

Privacy Notice

The school's privacy notice, in accordance with guidance provided by the Department for Education appears as appendix 2 to this policy. (Information about the school's Privacy Notice is made available to students and parents/carers via the school website and MyChild.

General Data Protection Regulation (GDPR)

GDPR becomes effective on 25th May 2018 and the school is getting ready for this. In due course, the school will appoint a DPO (Data Protection Officer) whose responsibilities include:

- Educating the school and its staff on important compliance requirements;
- Training staff involved in data processing;
- Conducting audits to ensure compliance;
- Serving as the contact point between the school and GDPR Supervisory Authorities;
- Monitoring performance and providing advice;
- Maintaining records;
- Interconnecting with data subjects and parents.

The ICO has prepared information about readiness for GDPR – the 12 step review will place the school in a position to be able to fully comply with the new requirements and these are:

1. Awareness;
2. Clarity about information we hold;
3. Communicating privacy information;
4. Individuals' rights;
5. Subject access requests;
6. Lawful basis for processing personal data;
7. Consent;
8. Children;
9. Data breaches;
10. Data Protection by Design and Data Protection Impact Assessments;

11. Data Protection Officers;
12. International (not relevant to school).

The Senior Information Risk Officer (SIRO)

All schools should have a senior member of staff who is familiar with information risks and the school's risk-reduction strategies. This is usually a member of the Senior Leadership Team and for our school the SIRO is the School Business Manager.

The SIRO must:

- Ensure appropriate mitigations are in place to minimise risk;
- Foster a culture that values, protects and utilises information securely and in a way that benefits the organisation;
- Take charge of the information risk policy and risk assessments and ensure that they are implemented by the Information Asset Owners;
- Act as an advocate for information risk management.

SIROs should seek to enhance their skills and capabilities, keeping up to date as is relevant for the organisation.

The Information Asset Owner (IAO).

The IAO is any member of the school team who is responsible for compiling or working with specific personal information. They must:

- Know what information the organisation holds and for what purpose;
- Understand how information is amended, added to, removed, or moved over time;
- Know who has access to the data and for what purpose;
- Recognise how the information is retained and disposed of securely.

Appendix 1

Dealing with a subject access request

- Requests for information must be made in writing (which includes the use of e-mail) and be addressed to the headteacher. If the initial request does not clearly specify the information required, then the school will make further enquiries.

- The headteacher must be confident of the identity of the individual making the request. When the request concerns data about a pupil, checks will also be carried out regarding proof of relationship to the child. In addition, evidence of identity will be established by requesting production of:
  - Passport.
  - Driving licence.
  - Utility bills with the current address.
  - Birth/marriage certificate.
  - P45/P60.
  - Credit card or mortgage statement (this list is not exhaustive).

- As stated above, any individual has the right of access to information held about them. However, in the case of children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.

- The school may make a charge for the provision of information, depending on the following:
  - No charge can be made if the requester simply wants to view the educational record of a child.
  - Should the information requested require a copy of the educational record, then the amount charged will be dependent upon the number of pages provided. This type of record is available to all parents until the child becomes an adult with or without the consent of the child. The school is required to respond within 15 school days.
  - Should the information requested be personal information that is not an educational record, schools can charge up to £10 to provide it.

- The response time for subject access requests, other than for educational records, is 40 calendar days from receipt (although there may be an unavoidable delay if the request is made during school holidays).

- The DPA allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

- Third party information is information that has been provided by another person such as the local authority, the police, a health care professional or another school. It is normal good practice to seek the consent of the third party before disclosing information. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed. (There is no need in the case of third party requests to adhere to the 40-day statutory timescale.)

- Any information that could cause serious harm to the physical, emotional or mental health of a pupil or another person may not be disclosed, nor should information that would reveal

that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.

- If there are concerns about the disclosure of information, then additional advice should be sought, usually from the Information Commission's Office.

- When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

- Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.

- Information can be provided at the school with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.

- Complaints will be dealt with in accordance with the school complaints procedure, which is available on-line or from the school office. Should the complainant wish to take the matter further, it may be referred to the Information Commissioner www.ico.gov.uk.

- This policy will be reviewed by the headteacher at least every two years.

Appendix 2

Privacy Notice – for parents, carers and pupils

(Information about the school's Privacy Notice is made available to students and parents/carers via the school website and MyChild)

Data Protection Act 1998: How we use pupil information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.

Once our pupils reach the age of 13, the law requires us to pass on certain information to Warwickshire County Council, who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that **only** their child's name, address and date of birth be passed to Warwickshire County Council by informing the school. This right is transferred to the child once he/she reaches the age 16. For more information about services for young people, please go to our local authority website www.warwickshire.gov.uk

Careers guidance – the school will pass young people's information to careers guidance services or the national careers service as required to facilitate the provision of guidance and/or advice as the request of students.

We will not give information about our pupils to anyone without their consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about the pupil that we hold, please contact the school office.

We are required, by law, to pass some information about our pupils to the Department for Education (DfE) and to our local authority. DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at www.warwickshire.gov.uk or
- the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Privacy Notices – for the school workforce: those employed to teach, or otherwise engaged to work at school

(Information about the school's Privacy Notice is made available to staff via the school noticeboard and MyLearning)

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body.

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority;
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

- the LA website – www.warwickshire.gov.uk
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

Simon Dilkes,
School Business Manager,
The Polesworth School.

Appendix 3

What is Personal Information?

Personal information is anything relating to a person that can be used to identify them. This includes both manual paper records and digital records.

In a school, examples of personal information include:

- Names of staff and pupils;
- Dates of birth;
- Addresses;
- National insurance numbers;
- School marks;
- Medical information;
- Exam results;
- SEN assessments and data;
- Staff performance management reviews.

This list is not exhaustive, but is given to exhibit the range of what might be described as personal information.