Pontefract Academies Trust

Freedom of Information and Data Protection Policy and Procedure

Trust Board Approval Date	15 March 2017
Effective Date	1 May 2017
Planned Review Date	1 May 2020
Web Access	Internet
Owner	Director of Finance, Business & Operations

Pontefract Academies Trust

Contents

		Page
1.	Purpose, Scope, and Definitions	1 - 2
2.	Fair Processing	3 - 6
3.	Information Security	7 - 11
4.	Freedom of Information Publication Scheme	12 - 17

1. Purpose, Scope and Definitions

1.1 PURPOSE

The purpose of this policy and procedure is to ensure compliance of the Pontefract Academies Trust ("the Trust") with all of its obligations as set out in the Data Protection (DPA) and Freedom of Information legislation (FOI).

Where this policy and procedure refers to the Trust it will be referring to information held and processed by the following schools in addition to that of the central Trust headquarters:

- Carleton Community High School
- Carleton Park J&I School
- De Lacy Primary School
- Halfpenny Lane Junior Infant & Nursery School
- Larks Hill Junior & Infant School
- Orchard Head J&I School
- The King's School Pontefract
- The Rookeries Carleton J&I School

1.2 DATA CONTROLLER

The Trust is the Data Controller as defined in the Data Protection Act 1998 and is registered with the Information Commissioners Officer (ICO) as registration number **ZA021300**. The details of this registration can be found on the following link to the Information Commissioners Office website:
https://ico.org.uk/ESDWebPages/Entry/ZA021300

The Trust will renew the registration annually in October of each year. If the Trust introduces any new purposes for processing personal information, then it will notify the ICO, requesting that the new purpose be included in the registration.

1.3 DEFINITIONS

1.3.1 **Personal data** is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

1.3.2 **Sensitive personal data** is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data

1. Purpose, Scope and Definitions

1.4 DATA PROTECTION PRINCIPLES

The eight core principles of the Data Protection Act are enshrined in this policy in the Trust's commitment that personal data:

- Is processed fairly and lawfully;
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- Is accurate and, where necessary, kept up to date;
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Is not kept for longer than is necessary for those purposes;
- Is processed in accordance with the rights of data subjects under the DPA;
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

2 Fair Processing

2.1 FAIR PROCESSING

The Trust is committed to being clear and transparent about what type of personal information it holds and how it is used.

2.1.1 Privacy Notice for Pupils and their Parents and Guardians

The Trust collects and holds personal information relating to it's learners and may also receive information about them from their previous school, academy trust, local authority and/or the Department for Education (DfE). This personal data is used to:

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

Once the Trust's learners reach the age of 13, the law requires it to pass on certain information to Wakefield M D Council who have responsibilities in relation to the education or training of 13-19 year olds. The Trust 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 Wakefield M D Council by informing the relevant school administrator. This right is transferred to the child once he/she reaches the age 16. More information about services for young people can be found on Wakefield M D Council's website http://www.wakefield.gov.uk/residents/schools-and-children/youth-support-services/youth-support-services-about-us

The Trust will not give information about its learners to anyone without parental consent unless the law and our policies allow it to do so. If a parent wishes to receive a copy of the information the Trust holds about their child they can request it from the administration team in their child's school

The Trust is required, by law, to pass some information about its learners to the Department for Education (DfE). This information will, in turn, then be made available for use by Wakefield M D Council.

The DfE may also share pupil level personal data that the Trust supplies 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

2 Fair Processing

requested and the arrangements in place to store and handle the data. To be granted access to pupil/student 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 can be found on:
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

Information on which third party organisations (and for which project) pupil/student level data has been provided to can be found on:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

For more information about how Wakefield M D Council and/or DfE collect and use informationcan be found on:

• Wakefield M D Council at http://www.wakefield.gov.uk/about-the-council/access-to-information/data-protection or

•the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

CCTV
Where CCTV is used by the Trust, it will only be for general security purposes in order to protect the learners and staff in each school.

Photographs
Pupil/Student photographs may be included, as part of their personal data and this will be treated with the same level of confidentiality as all other personal data.

Photographic images of pupils used in publically available media such as web sites, newsletters or the school prospectus will not identify pupils unless parental permission has been given in advance.

The Trust does not share any of its data with any other organisation without permission except where the law requires it. The Trust is required to provide pupil/student data to central government through the Department for Education (DfE www.education.gov.uk) and the Education Funding Agency (EFA www.education.gov.uk/efa). Where it is necessary to protect a child/student, the Trust will also share data with the Local Authority Children's Social Services and/or the Police.

Can a parent see the personal information held about their child?
All pupils/students have a right to have a copy of the personal information held about them. Pupils who are of primary school age cannot request a copy of their personal information it has to be made by their parent or guardian in writing. The only

circumstances under which the information would be withheld would be:

- if there was a risk that the information might cause serious harm to the physical or mental health of the pupil or another individual;
- Where disclosure would reveal a child is at risk of abuse;
- Information contained in adoption or parental order records;
- Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and
- Copies of examination scripts.

Making a Request for Personal Information about your child

Printed copies of personal data will be charged at the actual cost of providing the copy up to a maximum of a £10 charge. To protect each child's right of confidentiality under law the Trust reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed and any fee due paid, the information will be collected and provided within **40 calendar days**.

Copies of information that the Trust holds can be requested by emailing adminsupport@patrust.org.uk . Requesters should ensure letter/email title is detailed as "Subject Access Request".

Making a request for your child's educational record

All parents are also entitled to a copy of their child's educational record. A request must be made in writing to the relevant Headteacher/Head of School. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the academy. Only information that has come from a teacher or employee of the Trust or an educational professional contracted by the Trust can be considered to form part of the educational record.

The school will charge a fee to provide an actual copy of the educational record but this will not be greater than the actual cost of reproducing the information. Once any fee has been received the school will respond to the request within **15 school days** (21 calendar days excluding any public or academy holidays).

2.1.2 Privacy Notice for our Employees

The Trust processes personal data relating to those it employs to work at, or otherwise engage to work at our Trust. This is for employment purposes to assist in the running of the Trust 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

2 Fair Processing

- 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.

The Trust will not share information about our employees with third parties without their consent unless the law allows us to. The Trust is required, by law, to pass on some of this personal data to the Department for Education (DfE)

More information about how the Trust and/or DfE store and use personal data can be found on https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Copies of information that the Trust holds can be requested by emailing adminsupport@patrust.org.uk . Requests should ensuring letter/email title is detailed as "Subject Access Request".

3 Information Security

3.1 **Objective**

The information security objective is to ensure that the Trust's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

3.2 **Responsibilities**

The Headteacher/Head of School of each school has direct responsibility for ensuring that the staff in their school adhere to the information security requirements set out in this policy.

3.3 **General Security**

It is important that unauthorised people are not permitted access to Trust/school information and that all trustess/school governors/employees protect against theft of both equipment and information. This means that all trustees/school governors/employees must pay attention to protecting our buildings against unauthorised access.

Employees must:

a) Not reveal pin numbers or building entry codes to people that they do not know or who cannot prove themselves to be employees;
b) Beware of people tailgating them into the building or through a security door;
c) If a staff member does not know who someone is and they are not wearing some form of identification, the staff member should ask them why they are in the building;
d) Not position screens on reception desks where members of the public could see them;
e) Lock secure areas when vacating the area;
f) Not let anyone remove equipment or records unless certain who they are;
g) Visitors and contractors in Trust buildings should always sign in a visitor's book/system.

3.4 **Security of Paper Records**

a) Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
b) Records that contain personal data, particularly if the information is sensitive must be locked away when not in use and must not be left open or on desks overnight or when the responsible person is not in the office;
c) Responsible persons should always keep track of files and who has them;
d) Responsible persons should not not leave files out where others may find them;
e) Where a file contains confidential or sensitive information, it must not be given to someone else to look after.

3.5 **Security of Electronic Data**

Most of the Trust's data and information is collected, processed, stored, analysed and

reported electronically. It is essential that all Trust systems, hardware, software and data files are kept secure from damage and unauthorised access. Trust staff must:

a) Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;
b) Supplies of CDs containing software should be kept safe and locked away. CDs should always be clearly labelled in case they need to be re-loaded;
c) When buying a license for software, it usually only covers a certain number of machines. This number must not be exceeded as this will result in the terms of the contract being broken.
d) Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion by:
    - Not writing it down;
    - Not sharing individual passwords;
    - Using secure passwords which should be at least 8 characters (using a mix of numbers, lower and uppercase letters);
    - The essential rule is that your password is something that can be remembered by an individual but is not anything obvious (such as password) or anything that people could guess easily such as an individual's name;
    - An employee can be held responsible for any malicious acts by anyone to whom they have given their password;
    - Employees should change their passwords regularly, and certainly when prompted. Employees should change their passwords if they think that someone may know what it is.

Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

3.6 **Use of E-Mail and Internet**

The use of the Trust's e-mail system and wider Internet use is for the professional work of the Trust. Reasonable personal use of the system in an employee's own time is permitted but professional standards of conduct and compliance with the Trust's wider policies are a requirement whenever the e-mail or Internet system is being used.

The Trust uses a filtered and monitored broadband service to protect the Trust's learners. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Employees discovering such sites on the system must report this to their line manager immediately. The Headteacher/Head of School will ensure that the sites are reported to the broadband provider for filtering.

To avoid a computer virus arriving over the Internet, employees should not open any flashing boxes or visit personal websites;

Employees should not send highly confidential or sensitive personal information via e-

mail without encryption and/or password security;

Unimportant e-mails should be deleted straight away;

Employees must not send information by e-mail, which breaches the Data Protection Act.

Employees must not write anything in an e-mail which could be considered in breach of the Trust's Employee Code of Conduct, or Equality and Diversity Policy.

3.7 **Electronic Hardware**

All hardware held within Trust should be included on the school asset register or inventory;

When an item is replaced, the school register/inventory should be updated with the new equipment removed or replaced;

Employees must not let anyone remove equipment unless they are sure that the person is authorised to do so;

In non-secure areas, clamps or other security devices must be used to secure laptops and other portable equipment to desktops.

3.8 **Remote Working Guidance**

If employees must work outside of the Trust/School or at home, all of the 'Information Security' policy principles still apply. However, working outside of the Trust/School presents increased risks for securing information. The following additional requirements apply:

- Employees must not access confidential information when they are in a public place, such as a train and may be overlooked;
- Employees must not have conversations about personal or confidential information on their mobile phone when in a public place. They should ensure that, if urgent, then the conversation is held in a separate room or away from other people;
- If an employee uses a laptop or tablet or smart phone they should ensure that it is locked and pass-word protected to prevent unauthorised access;
- Employees must ensure that they do not leave their device anywhere it could be stolen. It should be kept with them at all times and be secure when in the Trust/school;
- Any portable device or memory stick that contains personal data must be encrypted. Personal data may not be taken off any Trust/school site or put onto a portable device without the express permission of the CEO/Headteacher/Head of School. Taking personal data off-site on a device or media that is not encrypted would be a disciplinary matter.

3 Information Security

The Headteacher/Head of School will make arrangements to maintain a register of:

- protected data that has been authorised for use on a portable device;
- the fixed period of time that the authorisation relates to;
- the reason why it is necessary to place it on the device;
- the person who is responsible for the security of the device and its data;
- the nature of encryption software used on the device;
- confirmation of the date that the data is removed from the device.

Employees working on confidential documents at home must

- not leave them lying around where others may see them;
- must dispose of documents using a shredder;

If an employee is using their own computer, they must ensure that others cannot access Trust/school documents/systems. When an employee has completed working on a document it should be transferred back to the Trust's system and deleted from the computer. It is strictly forbidden to use a computer owned by an employee to hold personal data about pupils or staff at the Trust/school.

3.9 **Audit of Data Access**

Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

3.10 **Data Backup**

The Trust will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the Trust is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

Data backup should routinely be managed on a rolling daily process to secure off-site areas.

3.11 **Disposal of Information**

Paper records should be disposed of with care. If papers contain confidential or sensitive information they should be shredded before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

Where a third party contractor holds personal information on behalf of the Trust, for example the payroll provider, the Trust will seek reassurance from the contractor regarding their data protection policies and procedures.

3 Information Security

3.12 **Websites**

Where personal information, including images, are placed on Trust websites the following principles will apply:

- Personal information (including photos) will not be disclosed on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;
- Regulations regarding cookies and consent for their use will be complied with;

3.13 **Processing by Others**

The Trust remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of the Trust will have to specify how they will ensure compliance with data protection law.

4. Freedom of Information Publication Scheme

Information to be published.	**How the information can be obtained (hard copy and/or website)**	**Cost**
Class 1 - Who we are and what we do		
Who's who in the Trust and its schools	Trust Website School Websites	Free
Who's who on the Members/ Trust Board / School Governance Committees	Trust Website School Websites	Free
Instrument of Government/Articles of Association/Funding Agreement	Trust Website	Free
Contact details for the CEO, Headteacher, Head of School and for the Trust Board, School Governance Committees via the Trust/schools (named contacts where possible).	Trust Website School Websites	Free
School prospectus (if any)	School Websites	Free
Staffing structure	Trust Website School Websites	Free
School session times and term dates	School Websites	Free
Address of school and contact details, including email address	Trust Website School Websites	Free

4. Freedom of Information Publication Scheme

Information to be published.	**How the information can be obtained (hard copy and/or website)**	**Cost**
Class 2 - What we spend and how we spend it		
Annual budget plan	Hard Copy	Free
Annual Report and Financial statements	Trust Website	Free
Capital funding	Hard Copy	Free
Financial audit reports	Hard Copy	10p/sheet
Details of expenditure items over £2000 – published at least annually but at a more frequent quarterly or six-monthly interval where practical.	Hard Copy	10p/sheet
Procurement and contracts the school has entered into, or information relating to/a link to information held by an organisation which has done so on its behalf (for example, a local authority or diocese).	Hard Copy	10p/sheet
Pay policy	Trust Website	Free
Class 3 – What our priorities are and how we are doing		
School profile	School Website	Free
Performance data supplied to the English Government, or a direct link to the data	School Website	Free
The latest Ofsted report	School Website	Free
Post-inspection action plan	Hard Copy	Free

4. Freedom of Information Publication Scheme

Information to be published.	**How the information can be obtained (hard copy and/or website)**	**Cost**
Performance management policy and procedures.	Trust Website	Free
Performance data or a direct link to it	Trust Website School Websites	Free Free
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status	Trust Website School Websites	Free Free
Safeguarding and child protection	School Websites	Free
Class 4 – How we make decisions		
Admissions policy/decisions (not individual admission decisions) – where applicable	Trust Website School Websites	Free
Agendas and minutes of meetings of the Trust Board and its committees. (NB this will exclude information that is properly regarded as private to the meetings).	Hard Copy	10p/sheet
Class 5 – Our policies and procedures		
Governance Policies Finance Policies HR Policies	Trust Website School Websites	Free

4. Freedom of Information Publication Scheme

Information to be published.	**How the information can be obtained (hard copy and/or website)**	**Cost**
Health and Safety at Work Policies Records management and personal data policies, including: • Information security policies • Records retention, destruction and archive policies • Data protection (including information sharing policies)		
Charging regimes and policies.	School Websites	Free
Class 6 – Lists and Registers		
Curriculum circulars and statutory instruments	Hard Copy	Free
Any information the school is currently legally required to hold in publicly available registers (THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER)	Hard copy	10p/sheet
Class 7 – The services we offer		
Extra-curricular activities	School Websites	Free
Out of school clubs	School Websites	Free
Services for which the school is entitled to recover a fee, together with those fees	Hardcopy	10p/sheet
School publications, leaflets, books and newsletters	School Webiste or on request from school	Free

4. Freedom of Information Publication Scheme

Information to be published.	**How the information can be obtained (hard copy and/or website)**	**Cost**
Additional Information		
Subject Access Requests	Hard Copy	10p/sheet

4. Freedom of Information Publication Scheme

SCHEDULE OF CHARGES

This describes how the charges have been arrived at.

TYPE OF CHARGE	DESCRIPTION	BASIS OF CHARGE
Disbursement cost	Photocopying/printing @ 10p per sheet (black & white)	Actual cost *
	Postage	Actual cost of Royal Mail standard 2nd class

* the actual cost incurred by the Trust