TRINITY ACADEMY NEWCASTLE TRUST

DATA PROTECTION POLICY

Approved by Resources Committee – Oct 2017

On behalf of the Board

Next Review Date – Oct 2018

Our Commitment:

Trinity Academy Newcastle Trust 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/data-protection-principles/

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The member(s) of staff responsible for data protection are: June Renwick Head of School (Business), Berjees Tata Data Manager

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.

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

Notification:

Our data processing activities will be 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 immediately to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

The principles of the Data Protection Act shall be applied to all data processed:

1. Processed fairly and lawfully

2. Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes

3. Accurate and, where necessary, kept up to date,

4. Adequate, relevant and not excessive in relation to the purposes for which it is processed

5. Not kept for longer than is necessary for those purposes

6. Processed in accordance with the rights of data subjects under the DPA

7. Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage

8. 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

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

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.

Records Management
Good Practice

Email

- Do not assume that email is confidential or secure
- Email may be subject to disclosure
- If in doubt, validate the sender of an email
- Use encryption to send strictly confidential emails
- Do not rely on email for record keeping

Sending Information

- If there is a need to send information via email contact the IT help desk at the Civic 0191 2777282

Disposal

- Place all office papers in the Shred bins /Admin Office
- Confidential or restricted waste on media other than paper should be physically destroyed, reformatted or securely wiped clean

Your desk and work area

- Confidential information on display should be kept to a minimum and only have data which is connected to the current work out on display
- Wherever possible all documents and computer media should be filed and locked away at the end of the day.
- If you leave your desk unattended, you must lock your machine by pressing CTRL+ALT+DEL

Answering Queries

- Do not give any information if you are at all unsure
- Use call back in order to validate a particular caller. This may need to be done by administrative staff at Trinity
- Do not speak to the Press. All queries should be directed to the CEO
- Any queries from the police must be accompanied by a Section 29 notice or court order

Passwords

- Do not share your password with others
- Change your password regularly
- Make your password unique – do not use birthdays or names of close family members

Awareness

- All staff should report immediately any observed or suspected security incidents where a breach of any of the trust policies has occurred, any security weaknesses in, or threats to, systems or services

Working from home

- Remote access via Azure Multi-Factor Authentication (MFA)
- **Use of a USB devise is not permitted unless an Iron key and permission must be granted by Senior Leadership Team**
- All incidents involving the use of home working facilities must be reported immediately

Your devices must be physically secure when unattended

- Keep information on your device to a minimum
- Do not leave any Trinity equipment unattended in your car
- Do not carry devices and access codes in the same bag
- Always lock up your tablet/laptop/Ipad overnight
- Guard against thieves when travelling – taking extra care at times and in places where you can become distracted
- Only take records off site where it is absolutely necessary and sign and date when they have been taken
- Always transport records in a secure way
- Do not leave records unattended, especially if they can be viewed by a member of the public
- Return records when no longer needed off-site and log that they have been returned. This log should be signed and dated by the person returning the records
- If you are working from home – under no circumstances send work related emails using your home email accounts

Data Protection and the Safeguarding of Children and Young People
Keep all child protection notes together in a secure place i.e. a locked cabinet.

Guidance

- Some daily information may not be suitable for the Tracking Sheet or may be of a confidential nature. This will be kept confidentially by Admin Officer in confidential file.
- Extended family members should be kept together or cross referenced.
- Place a note or symbol on the child's academy file to denote that a child protection file is held for the child.
- For each child protection record for a child ensure that the file has a facing sheet inside the file which records:
  - The child's full name
  - Date of birth
  - Address
  - Name and address of GP
  - Information about family members
  - An indication of where a piece of information is, if it has been 'lifted' from the file for some reason
  - A note if there is more than one file for the child

Who should have access to child protection information?

- Should be on a 'need-to-know basis among the staff
- Notes are not shared with families, except for child protection reports to the child protection case conference.
- Other statutory agencies (e.g. not solicitors)

What happens to the information when the child leaves your academy?
If a child for whom there have been child protection concerns (whether registered or not) is moving to another academy:

- The whole child protection file should be sent, separately from the academy file, to the receiving academy.
- The file should be marked 'confidential, addressee only' and should be sent to the Head teacher of the receiving academy.
- As extra security, space permitting, keep a copy of the sent file as ‘dormant’, in case the original gets lost in transit.
- Give the name and contact number of the key worker (from Social Services) who dealt with the family if applicable.
- If you do not know details of the receiving academy, wait 21 days for the academy to contact you. If you hear nothing by then, contact your Designated Officer for Child Protection for advice.

How long should records be kept?
For a child leaving secondary academy, child protection records should be kept until the child reaches the age of 24.

Source
Information Security “It’s everyone’s responsibility” - Information Governance Team Room 245 (Newcastle City Council) – Contact Sarah Graham at 0191 2777668
sarah.graham@newcastle.gov.uk
Data Protection Policy Newcastle City Council
Safeguarding Children Policy for Academys – Education Welfare Services Newcastle

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy-impact-assessments-code-published/

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 these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 40 days and they should be made in writing to: June Renwick Head of School (Business)

A charge may be applied to process the request.

https://ico.org.uk/media/for-organisations/documents/1586/personal_information_online_small_business_checklist.pdf
https://ico.org.uk/media/for-organisations/documents/1235/definition-document-schools-in-england.pdf

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.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

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/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Insert link to relevant page on IT asset disposal partner's website, e.g.
https://www.stonegroup.co.uk/contact/book-recycling-collection/

Signed on behalf of the Governing Body:

_____

Peter Carter (Chairperson of the Board)

Date: 11.10.17