Northumberland County Council

shortstay Northumberland's P.R.U.

Reviewed: April 2017

Data Protection Policy

RATIONALE

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. The Data Protection Act gives individuals certain rights regarding information held about them. It places obligations on those who process data while giving rights to those who re the subject of their data. Personal information covers both facts and opinions about the individual. Northumberland PRU follows the guidance of the Northumberland LA's Data Protection Policy.

PURPOSE

Information is:

- held securely and confidentially
- obtained fairly and lawfully
- recorded accurately and reliably
- used effectively and ethically
- shared appropriately and legally

This covers all information and everyone is responsible for it, and must comply with guidance and legislation from a number of sources.

Good Practice

Anyone processing personal information must comply with eight enforceable principles of good information handling practice. These say that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than necessary
- processed in accordance with the individual's rights
- secure
- not transferred to countries outside EEA unless country has adequate protection for the individual

Information Classifications

There are four security classifications:

- confidential
- restricted – any material that links any identifiable information which, if released, would cause serious or significant harm or distress
- protect – compromise of information would be likely to affect individuals in an adverse manner
- unclassified – information that is destined for the public

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:

- refer to the Information Asset Classification Policy (LA) for guidance on the level of protection needed for various types of information

Disposal:

- place all papers containing personal information in the 'Shred It' bins (main office & reprographics) – this paper is then shredded by the Company employed by the PRU.
- 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, 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 Northumberland PRU. Do not speak to the Press. All queries should be directed to The Press Office at the County Hall via the Head teacher
- 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 you password unique – do not use birthdays or names of close family members

Awareness:

- all staff should report immediately any observed or suspected security incidents

Working from home:

- 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 Northumberland PRU equipment unattended in your car
- do not carry devices and access codes in the same bag
- always lock up your laptop 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

CCTV:

- see CCTV Policy for details regarding data protection of CCTV images

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 pupil files or may be of a confidential nature.
- extended family members should be kept together or cross referenced
- place a note or symbol on the child's school 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

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 school?

If a child for whom there have been child protection concerns (whether registered or not) is moving to another school:

- the whole child protection file should be sent, separately from the school file, to the receiving school
- the file should be marked 'confidential, addressee only' and should be sent to the Designated Person for CP of the receiving school
- 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 school, wait 21 days for the school 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 school, child protection records should be kept until the child reaches the age of 24.

Source

Information Security "It's everyone's responsibility"
Data Protection Policy Northumberland Council
Safeguarding Children Policy for Schools – Education Welfare Services

_____ **Chair**

_____ **Date**