St Catherine's C of E Primary School

Data Protection and Password Policy

Introduction
The Data Protection Act is designed to protect the privacy of individuals and to ensure that personal data is processed fairly and lawfully.
It protects personal data by setting terms and conditions that all staff must follow when processing details about any living individual. You can read about these in section 7 of the Act.

What is 'Personal Data'?
Personal data is anything that identifies a living person and includes:
• a name and address, telephone number
• financial information
• a national insurance number
• a birth certificate
• a passport
• a driving licence
• a personal email address
• CCTV images
• sensitive details, such as religion, health records, or ethnic origin

What is 'Sensitive Personal Data'?
Sensitive personal data is identified separately in the Act because further conditions need to be applied before it can be used.

Explicit consent from the person concerned is required before those details can be shared or passed to others in order to provide a particular service.
Of course there are times when our 'duty of care' or legal duty requires us to inform others, perhaps for example, following an assessment of identified risks relating to a specific individual.

Data Protection Act 1998
The Act sets out terms and conditions for processing personal data.
• The 8 principles provide the framework of the legislation.
• The County Council has a Data Protection Policy which requires staff to work according to the Principles.

Rights of individuals provided by the Act
Everyone has the right to access their own personal data, to be sure the information held by an organisation is correct, to know the purpose it is being used for and if it is being shared with any third parties.

• Employees of Cornwall Council have the right to access their personal data, which is held for employment purposes. (This does not include information processed by staff as part of their role at work)

• Staff will need to speak to their manager or H.R. representative if they wish to see their own personal records and if circumstances change, e.g. move home, it is the staff member's responsibility to notify their Manager in order to maintain accuracy of the information that is held.

▪ Parents/Primary Carers and Legal Guardians hold the responsibility of informing schools if their child(ren)'s home/and or contact details change.

What Are The Eight Principles of the Act?

All employees of Cornwall Council must process data in accordance with the Eight Principles of the Data Protection Act.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

a.) at least one on the conditions in Schedule 2 is met, and

b.) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (conditions in Schedules 2 and 3 – found at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is being processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of the data subjects under this Act.

7. 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.

8. 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.

Applying to see personal data- Subject Access Request (SAR)

- Members of the public requesting disclosure of their own personal data held by the Council must complete the relevant form. This needs to be returned together with evidence of identification along with the fee to the Data Protection Officer
- Current staff are not required to pay the fee and can make an informal request through their manager or H.R. representative.

Protecting Yourself

If as an employee of Cornwall Council you do not wish to receive advertising literature through direct mailing, you also have the right to inform the data controller (Organisation) in writing, and to agree a reasonable time limit for this to cease.

Staff can also ensure that their telephone number is no longer available to organisations, including charities and voluntary organisations who may telephone staff with offers and information they do not wish to receive.
This can be done by contacting the company directly or you can register with a central register – the Telephone Preference Service. (This is a free service)

Processing different types of personal data
The Council has a Data Protection policy all staff are required to comply with when processing personal data as part of their role at work.
Processing includes things such as:
• recording and updating personal details
• recording information from telephone calls
• reviewing the file (paper or electronic)
• reading the file or documents
• storing/archiving the file or documents for future use
• discussing any action that needs to be taken
• creating/receiving e-mails or other correspondence

Using a form to collect personal data
Collecting personal details using a form (manual or electronic) requires staff to create a 'fair obtaining statement' clearly setting out the purpose it will be used for, who it may be shared with, and if the data is to be stored electronically this must be explained.
If you wish to send further information to the person in the future e.g. promotional literature, you must obtain consent to do so.
The person can then make an informed decision about whether or not they wish to complete the form and clearly understands how and why their details will be processed.

Collecting personal data over the telephone
When staff record names and addresses over the phone in order to answer a query or provide details of one of the County's services staff must make sure the person understands why staff are recording their details, and that it may be necessary to pass contact information to another department.
If staff use an answer-phone to collect enquiries eg. for job application forms staff need to be open and fair. E.g. personal details will only be used to process requests for an application form. They will not be used for any other purpose or passed on to other organisations.

Who to contact?
Each Council department has a Data Protection Co-ordinator, who should be the first point of contact for any query.

Your responsibilities as an employee of Cornwall Council
As an employee, *staff are legally obliged to process data fairly and lawfully, according to the terms and conditions of the Act*.
Staff are required to work according to the Council's Data Protection Policy, which includes the 8 principles of the Act.

Fines could result if staff knowingly process or misuse personal data without the consent of the employer, or parent/guardian of a child attending the school to third parties previously not highlighted in prior written communications.

Password Policy

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission.

Access to staff /admin accounts is only via a username and password. The passwords are changed every 90 days by the user. Any data taken off site not on a school computer is encrypted. This includes memory sticks and external hard disks.

Responsibilities

The management of the password security policy will be the responsibility of ICT Technician and ICT co-ordinator.

All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users can be allocated by the ICT Technician and ICT co-ordinator.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's data protection policy
- through the Acceptable Use Agreement form

Pupils / students will be made aware of the school's password policy:

- in computer and online safety lessons
- through the Acceptable Use Agreement form

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager / ICT coordinator and will be reviewed, at least annually, by the Online Safety Committee.

The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

Your Responsibilities – Data Security

Staff are responsible for ensuring the security of personal data.

- Requests from outside agencies and third parties for disclosure of personal information must not be processed. Resultant queries from staff must be made to the data protection coordinator directly and staff must have the direct permission to act when releasing or forwarding personal data.
- Staff should never give anyone passwords, or write it down for others to find or choose a password that could be guessed easily.
- Staff should never leave information about people on their desk when it is not being used.
- Filing cabinets should be kept locked and the keys held in a safe place.
- Staff will follow all set working procedures as their job involves processing personal details relating to staff, governors, children and associated parents and guardians.

Guidelines to help our school comply

Notification – make sure we notify the ICO accurately of the purposes for processing of personal data.

Personal data – we recognise the need to handle personal information in line with the data protection principles.

Fair processing – we can inform pupils and staff about what we do with the personal information we record about them. We make sure we restrict access to personal information to those who need it.

Security – we keep confidential information secure when storing it, using it and sharing it with others.

Disposal – when disposing of records and equipment, we make sure personal information cannot be retrieved from them.

Policies – we have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation.

Subject access requests – we will recognise, log and monitor subject access requests.

Data sharing – we make sure we are allowed to share information with others and make sure it is kept secure when shared.

Websites – we control access to any restricted area. We make sure we are allowed to publish any personal information (including images) on our website.

Photographs –when our school takes photos for publication, we mention our intentions in our fair processing/privacy notice.

Processing by others – we recognise when others are processing personal information for us and make sure they do it securely.

Training – we update staff and governors in the basics of information governance; recognise where the law and good practice need to be considered; and know where to turn for further advice.

Freedom of information – after consultation, we notify staff what personal information we would provide about them when answering FOI requests.

School Responsibilities – Stored Data

All Cornwall Council departments and schools have a Retention Policy which provides timescales for different types of records.
When data is 'historic' all departments should consider whether to destroy, file or archive the document according to the retention requirements.

For further advice and information on Data Protection, go to
www.ico.org.uk

Review Date : Annually