Cairney School

Personal Data Protection Policy

August 2015

Cairney School
Personal Data Protection– Policy Statement

Cairney School recognises and accepts its responsibility as set out in the Data Protection Act 1998 and sub-legislation contained therein. Cairney School will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information and to comply with the Data Protection Principles set out in the 1998 Act.

The following information provides an aid to the Data Protection Act 1998 and the material can be accessed via ALDO (Aberdeenshire Learning and Online Development); every employee of Aberdeenshire Council involved in the handling of personal data must complete the training on ALDO.

DATA

Any information held, or likely to be held by the Council, which relates to and can "identify" a living individual is considered to be "personal data". This includes any expressions of opinion about an individual.

Any information concerning deceased individuals is NOT covered by the Data Protection Act.

It is not always straight-forward to determine whether information is personal, or not.

A name is not always necessary for information to be considered, "personal". For example, a postcode on its own could be considered personal data, if that postcode relates to a single household with a single occupant i.e. if it relates to an identifiable living individual.

For information to be personal, it must have an individual as its focus and be significantly biographical about an individual.

Practical examples follow:

Information concerning Queen Victoria would not be personal information as Queen Victoria is not living.

The name John Smith together with the fact that this individual lives in the UK, would not alone be personal information as there are lots of John Smith's living in the UK and this does not uniquely "identify" the individual.

SENSITIVE PERSONAL DATA

There are eight categories of personal information considered to be "sensitive".

You must satisfy a Schedule 3 condition, to process sensitive personal information.

The eight categories of sensitive personal information are:

- Information concerning an individual's racial or ethnic origin
- An individual's Political Opinions
- An individual's Religious Beliefs
- Information concerning an individual's Trade Union membership
- Information about an individual's Physical or Mental health
- Information about an individual's Sex life
- Information about an individual's commission of offences
- Information about proceedings for any offences committed by an individual

Practical examples follow:

The fact that John Doe is a Buddhist is sensitive personal information.

The fact that Jane Doe suffers from asthma is sensitive personal information.

The fact that Jimmy Doe votes for the Conservative Party is sensitive personal information.

PROCESSING

The term “Processing” covers pretty-much everything that can be done with personal information.

- You process personal information if you obtain it.
- You process personal information if you record it.
- You process personal information if you hold it.
- If you organise, adapt or alter the data you are processing it.
- If you retrieve, consult or use the data you are processing it.
- If you disclose the information you are processing it.
- If you align, combine, block, erase or destroy the information, guess what, … you are also processing it.

DATA SUBJECT

The Data Subject is the individual who the data is about.

If Human Resources hold a staff file about John Doe, John Doe is the data subject. If the personal data is about you, you are the data subject.

DATA CONTROLLER

Where Aberdeenshire Council determines the purposes for which, and the manner in which, personal information will be processed, it is the “Data Controller” of that information.

The Data Controller is the legal entity responsible for complying with the Data Protection Act.

Scottish schools are not Data Controllers in their own right.

Aberdeenshire Council is the Data Controller of all schools within Aberdeenshire.

Practical examples follow:

If the Aberdeenshire Council Housing and Social Work service were to collect information for the purpose of “establishing housing requirements for tenants”, then “Aberdeenshire Council” is the Data Controller of this information.

If Turriff Academy were to collect information for the purpose of “arranging a school trip”, “Aberdeenshire Council” is the Data Controller of this information, as Turriff Academy is not a legal entity.

DATA PROCESSOR

A Data Processor is any person, other than an employee of the Data Controller who processes personal information on behalf of the Data Controller.

Data Controllers sometimes use a Data Processor to process their data due to time and cost savings involved. A person is a Data Processor where it merely acts on the instructions of the Data Controller when processing personal data and does not determine any of the purposes itself.

A Data Processor has no statutory obligations under the Data Protection Act. If a Data Processor loses personal data, the Data Controller will be held responsible under the Data Protection Act.

A practical example follows:

Aberdeenshire Council contract with Joe Bloggs Ltd, to carry out a staff survey on behalf of Aberdeenshire Council. The Council has determined the purpose – it is the Data Controller. Joe Bloggs Ltd merely act under the instruction of Aberdeenshire Council – it is a Data Processor. If Joe Bloggs Ltd lose any personal data, Aberdeenshire Council would be held responsible under the Data Protection Act.

THIRD PARTY

A third party is any person other than an employee of the Data Controller or an employee of a Data Processor.

If Aberdeenshire Council were to pass personal information to NHS Grampian, for NHS Grampian to use for their own purposes, this would be disclosing information to a third party.

PRINCIPLES OVERVIEW

The eight Data Protection Principles form the backbone of the Data Protection Act.

They consist of a number of obligations with which Aberdeenshire Council must comply when processing personal data. The importance of the Principles is made clear by the powers which the Information Commissioner can use to enforce compliance with the Principles and also to issue fines for breaching the Principles.

It is really important that you understand and comply with the Principles.

PRINCIPLE 1

FAIRNESS

To ensure “fairness”, individuals must not be misled or deceived about what you do, or what you intend to do, with their personal information. You must tell an individual what you intend to do with their information, usually at the time their information is collected. You must tell an individual if you intend passing their information on to any other companies or organisations and you must tell an individual who you are i.e. that you are “Aberdeenshire Council”. If you are collecting information for use within a school, you must still tell an individual that you are “Aberdeenshire Council”.

Processing will be “unfair” if you use an individual’s data for something you have not told them about. Processing will be “unfair” if you pass an individual’s data onto another company or organisation without first making them aware that this could happen and processing will be “unfair” if you do not tell an individual who you are i.e. “Aberdeenshire Council”.

Practical examples of unfair processing include:

Telling an individual that you will use their data for the purpose of “Collecting Council Tax” and then using this same data for the purpose of “Collecting Waste”, without first telling them about this additional purpose.

Telling an individual that you are “Peterhead Academy” but not telling them that you are “Aberdeenshire Council”.

Passing an individual’s data onto a Housing Association without first telling them that this could happen.

LAWFULNESS

To ensure “lawfulness”, you must not break any laws in using an individuals’ personal information.

You must not breach the Computer Misuse Act, for example by collecting information via unauthorised access to a computer system. You must not breach the Human Rights Act, for example by not respecting an individual’s right to a private and family life, their home and correspondence. You must not breach “Confidentiality”, by passing on sensitive information that was provided to you with an expectation of confidence.

Practical examples of unlawful processing include:

Accessing the Council Tax system to gain information for your own personal use or for any other unauthorised use.

Passing on a sensitive employment reference that was provided to you with an expectation that it would be kept “confidential” i.e. not passed on.

THE SCHEDULES (2 & 3)

“Schedule 2” is the name given to a list of “conditions for using personal information”.

These conditions include:

- having an individual’s **consent** to use their information
- having a contract with an individual to use their information
- if it is in an individual’s “vital interests” i.e. life or death situation
- if a law permits use of the information

If you cannot satisfy one of the conditions set out in “Schedule 2”, you cannot use an individual’s personal information.

“Schedule 3” is the name given to a list of “conditions for using sensitive personal information”.

If you cannot satisfy one of the conditions set out in “Schedule 3”, you cannot use any sensitive information belonging to an individual.

Practical examples of satisfying a Schedule 2 or 3 condition include:

Having consent from an individual to use their data for the purpose of “arranging school transport for pupils”.

Using information for the purpose of “collecting Council Tax” or “provision of Social Care”, both of which are permitted and required by law.

PRINCIPLE 2

Everything that you do, or intend to do, with an individual’s personal information must be “specified” to them.

If you intend using an individual’s information for Purpose A, Purpose B and Purpose C, you must inform them of Purpose A, Purpose B and Purpose C.

If you collect information from an individual using a paper form, your intended uses of their information must be specified to them either on the form itself, or on a separate sheet.

If you collect information from an individual via the telephone, your intended uses of their information must be specified to them verbally.

If you intend capturing information electronically, e.g. via a CCTV system, you must display a notice informing individuals of the uses of their information.

Practical examples of this include:

Telling an individual that their telephone call may be recorded for training purposes.

Telling an individual, via a CCTV notice, that their information will be used to prevent and detect crime.

Telling an individual on a paper form that their information will be used to “establish their housing requirements” and “for research purposes”.

PRINCIPLE 3

On collecting personal information from an individual you must ensure that you do not collect more information than is necessary. Any information that you do collect must be adequate, relevant and must not be excessive for the purposes that you have already “specified” to the individual.

Prior to collecting information from an individual, work out the minimum information that you need to collect in order to fulfil your specified purposes.

Always question the need for each piece of information i.e. do I really need to ask for this?

Practical examples are:

Do not collect an individual’s telephone number if you have no requirement to ever call them.

Do not collect information about an individual's age, if you have no requirement to know their age.

Do you need to collect an individual's full address? Would knowing their postcode suffice, would knowing the first four characters of their postcode suffice?

PRINCIPLE 4

On collecting information about an individual, you must ensure that any information you collect, and hold, is accurate. You must also ensure that, where necessary, this information is kept up to date.

This is particularly important when documenting any opinions about individuals.

Under most circumstances, it is important to ensure that information is kept up to date, for example ensuring that an individual's contact details are current. However, there are limited circumstances where it is also important to keep out of date information, for example where you wish to maintain a historic record.

Practical examples include:

Sending sensitive Social Work correspondence to an out of date or incorrect address could ultimately lead to a substantial fine being received.

Failure to keep Housing Benefit information up to date could result in individual's receiving more or less benefits than they are entitled to.

PRINCIPLE 5

Any information that you collect about an individual must only be kept for as long as necessary.

An organisation must determine and set out appropriate retention periods for different classes and categories of information.

For some types of information, retention periods can be set in law. For other types of information, it is up to the organisation to determine an appropriate retention period, and/or to follow "best practice".

Retention periods can vary from a few days or weeks to 100 years, depending on the purpose for which the information was obtained.

When information reaches the end of its specified retention period, it must be securely destroyed, for example via Confidential Waste or via a cross-cut shredder. Under no circumstances should personal information be disposed of in normal waste or recycled waste.

If you have any questions concerning retention periods within Aberdeenshire Council, please contact the Council's Information and Records Manager.

Practical examples include:

Unsuccessful job applicant interview notes should be kept for six months and then securely destroyed thereafter.

Information concerning looked after children should be kept for one hundred years.

PRINCIPLE 6

Individuals have a number of rights with regard to the information that the Council holds about them.

An individual has a “Right of Subject Access”. An individual can write to the Council to request a copy of some, or all, of the personal information that the Council holds about them.

An individual has a “Right to Prevent Processing for Direct Marketing”. An individual can write to the Council to require that the Council stops using their information for marketing purposes. This is an absolute right that the Council must comply with.

An individual has a “Right to Rectify, Block, Erase or Destroy” information. An individual can write to the Council requesting that the Council rectifies, blocks, erases or destroys information about the individual. On receiving such a request, the Council must write back advising whether it intends to comply with the request or not.

An individual also has rights with regard to

- automated decision making;
- a right to prevent processing likely to cause damage or distress;
- a right to seek compensation;
- a right to complain to the Information Commissioner.

A practical example of this includes:

John Doe writes to the Council requesting that the Council rectifies two errors in his Social Work file. The Council reviews the request. The Council agrees to rectify the section of the file where it is in agreement with John Doe that the file is erroneous. The Council does not agree to rectify the section of the file where it is not in agreement with John Doe. Instead the Council supplements this part of the file, with a record of John Doe’s opinion. The Council writes back to John Doe within 21 days advising John Doe of the outcome of his request.

PRINCIPLE 7

Principle 7 is about security.

The Council must put in place appropriate measures to ensure that any personal information it holds is not accidentally lost, destroyed or damaged. These measures must also prevent any unauthorised or unlawful use of the information.

Organisational measures include having policies, procedures and guidance in place concerning the use of personal information and also provision of awareness training for all staff who use personal information in their work.

Technical measures include a wide range of things such as ensuring every device that contains personal information is encrypted - this includes, but is not limited to, laptops, flash drives and SmartPhones; ensuring that all staff use a sufficiently-long, complex password; ensuring that secure email is used where necessary; ensuring that laptops are not left in open view in cars; etc.

However, the Data Protection Act doesn't just apply to information held on electronic devices; it also applies to information held on paper.

Further technical measures to cover paper records include having a clear desk policy; keeping personal information in a locked filing cabinet; transporting paper records only where necessary and if doing so appropriately looking after the papers; where necessary using recorded delivery; etc.

Breaching Principle 7 could result in the Council receiving a fine of up to £500,000.

Practical examples of complying with Principle 7 include:

- *Always use a Council-provided, encrypted flash drive. Use of personally-owned flash drives is prohibited.*
- *Always use a long, complex password and change it regularly*
- *Always remember to put personal information back in a lockable filing cabinet before leaving work.*
- *Always lock your workstation (Ctrl-Alt-Del, Lock Workstation) when going away from your desk.*
- *Always treat Council assets and information appropriately. Look after them as if they were a bundle of cash.*

PRINCIPLE 8

Not all countries have laws equivalent to the Data Protection Act and not all countries respect Human Rights and privacy.

It is therefore important that personal information is only ever passed to countries which do have a law equivalent to the Data Protection Act and do respect Human Rights and privacy.

It is considered "safe" to pass personal information to any country in the European Economic area (which is basically European Union countries plus Norway, Liechtenstein and Iceland), as all of these countries do have Data Protection law.

There are only nine other countries in the world deemed "safe" from a Data Protection viewpoint.

The United States of America does not have an equivalent law to the Data Protection Act. Personal information can only be passed to a company in the United States, where that company has something called "Safe Harbor" status.

If an individual provides you with consent to pass their information to an unsafe country e.g. China, then you will not breach Principle 8.

You may think, "I would never pass personal information to another country". But is that actually true? What about when you use the internet?

Practical examples follow:

Have you ever filled in an online survey using Survey Monkey? Where is that information now located?

The answer is the United States of America. Survey Monkey does however have Safe Harbor status. Therefore, passing personal information to Survey Monkey would not breach Principle 8

SUBJECT ACCESS

Principle 6 of the Data Protection Act provides an individual with a number of rights – one of these rights is the right of Subject Access.

An individual can write to the Council requesting a copy of some, or all, of the information that the Council holds about them.

This type of request is called a "Subject Access Request".

The request MUST be in writing. A valid request can take the form of a Subject Access Request form, a letter or an email).

The individual MUST pay the necessary fee – which can be a maximum of £10.

The individual must also prove that they are who they say they are.

On receipt of a written request, the fee AND proof of identity, the Council must provide the individual with a permanent copy of the requested information, unless the individual agrees otherwise. The Council must provide the information PROMPTLY and in any event within 40 calendar days.

All information provided must be "intelligible", so any codes about the individual must be explained to the individual.

Individuals are not entitled to receive information about others. If their file contains any information about other individuals, this should be removed (or redacted) prior to providing a copy of the file to the individual.

Any other exempt data must also be withheld, for example, any information protected by Legal Professional Privilege, information provided to the Council by the Children's reporter, the Police, etc.

FAIR PROCESSING NOTICES

An individual must be provided with a Fair Processing Notice, also known as a privacy notice, generally in advance of processing their information.

A fair processing notice can be in writing

for example on a data collection form or on a notice alerting individuals to the use of CCTV

or verbal

for example when call centre staff advise that "your call may be recorded for training purposes".

A fair processing notice has several mandatory elements.

A fair processing notice MUST state the name of the Data Controller i.e. Aberdeenshire Council.

A fair processing notice MUST list all the purposes for which the information will be used.

And

A fair processing notice MUST provide any further information necessary for the processing to be considered "FAIR". This includes telling individuals about who you may pass their information onto, advising individuals that they have a right to withdraw consent and advising individuals that they have a right of subject access, etc.

NOTIFICATION

The Information Commissioner's Office manages and maintains a national register of all UK data controllers. The national register is accessible to the public, providing details of what information is processed by each and every Data Controller.

Only information held electronically needs to be notified. Any information held solely in paper form, does not need to be notified.

If you wish to collect personal data for a new purpose, and store that information electronically, it is essential to check the Council's register entry to ensure that your new purpose is already listed there.

If your new purpose is not listed you MUST make the Data Protection Officer aware prior to commencing processing. Failure to notify the Information Commissioner of any required changes to the register entry is a criminal offence.

Any required changes must be notified to the Information Commissioner's Office within 28 days of commencing processing.

The notification fee is £35 per annum, except for large organisations such as Local Authorities where the annual fee is £500.

CONSENT

Consent is one of the conditions in Schedule 2 which permits you to process personal information. Consent is also one of the conditions in Schedule 3 which permits you to process sensitive personal information.

If you have consent from an individual you may process their personal information. If you have explicit consent from an individual, you may also process their sensitive personal information.

Explicit consent is usually demonstrated by having an individual sign a consent form.

The downside to relying on consent, for processing personal information, is that consent can be withdrawn at any time and consent can be time-limited.

When seeking consent it is important to be honest about the purposes that the information will be used for and to not mislead or deceive the individual.

It is important that the individual understands what they are consenting to and is given appropriate time and privacy to reach any decision.

The individual should also be made aware of any outcomes or risks should they refuse to provide consent.

EXEMPTIONS

The Data Protection Act contains a considerable number of exemptions where certain specified types of information are exempt from one or more of the Data Protection Principles and/or are exempt from specified Sections of the Act.

Exemptions exist to ensure that the Data Protection Act cannot be used to obstruct the carrying out of functions such as the prevention and detection of crime, the assessment and collection of taxes, national security and the provision of a Social Work service.

A comprehensive understanding of all of the exemptions is outwith the scope of this course. If you require further information concerning exemptions, please contact your Data Protection representative in the first instance.

Practical examples follow:

The Data Protection Act must never be quoted as an obstacle to necessary child protection data *sharing. The Act contains an exemption with permits processing without having to inform individuals that you are processing their information and also removes the right of the data subject to request their information via subject access. This exemption applies where there is any risk of physical or mental harm to the individual or to any other person.*

Where a child is believed to be at risk, you will not breach the Act by sharing this information with relevant partner agencies e.g. the Police.

The Data Protection Act does not prevent parents from taking photographs or videos while attending school events such as school sports days and school concerts. The school is not the Data Controller of such information, the parent taking the photographs or doing the filming is the Data Controller. The school has no right to prevent parents from taking photographs unless the school believes this could result in a child protection issue. Data Protection must not be incorrectly quoted as justification for stopping parents from taking photographs or filming such events.

SECURITY

It is really important that you keep all personal information “secure”.

Failure to keep personal information “secure” could result in a fine of up to £500,000 being imposed on the Council.

Principle 7 of the Data Protection Act requires that technical and organisational measures be taken to prevent accidental loss, damage or destruction to personal information and to prevent unauthorised access to personal information.

Organisational measures include having appropriate Policies and Procedures in places for handling personal information. Organisational measures also include provision of Data Protection Awareness Training to all staff who process personal information.

Technical measures include using complex passwords to secure the information, using encryption software to secure the information, setting access rights appropriately, etc.

The requirement to keep personal information secure does not only apply to information held electronically. It is equally important to ensure that you keep paper records secure too.

The Council has a number of policies, procedures and guidance, located on the Council intranet, which you should ensure you remain familiar with.

Practical examples follow:

Never insert a personally-owned flash drive into a Council computer. Council approved flash drives with encryption software must always be used.

Never leave a Council laptop unattended in open view in a car and never leave a laptop in a car overnight.

If sending personal information via email ALWAYS ensure you are sending the minimum amount of information necessary and are sending it to the correct addresses. Check, check and check again!

Always ensure you dispose of paper records containing personal information into confidential waste.

ENFORCEMENT

The Information Commissioner is tasked with enforcing Data Protection law across the UK.

The Commissioner has a number of powers under the Act, including powers to assess and enforce the law.

An individual has the right, under Principle 6, to complain to the Information Commissioner requesting that the Commissioner assesses a Data Controller's compliance with the Act.

The Commissioner may serve an Information Notice on a Data Controller to provide the Commissioner with requested information.

It is a criminal offence to fail to comply with an Information Notice.

If the Commissioner is satisfied that a Data Controller is breaching, or has breached the Act, he may serve an Enforcement Notice requiring that the Data Controller takes specific steps to rectify the breach, within a limited time period.

It is a criminal offence to fail to comply with an Enforcement Notice.

The Commissioner also has the power to fine a Data Controller for breaching any of the Data Protection Principles, where the breach has resulted in substantial damage or distress to individuals. The fine can be up to a maximum of £500,000.

Date of Original Policy: August 2015

Revision No.	***Details of Change***	***Date***
1	Next Policy review	August 2016
2		
3		

Do you have any comments to make regarding this policy?

Signed _____ *Date* _____

Name (please print) _____

Please remove and return to the Head Teacher Cairney School