Data Protection Policy [006]

PILGRIM PATHWAYS SCHOOL

Cambridgeshire County Council

As an organisation that sits within CCC we are bound by the Data Protection Policy that sits below.

Approved by:	Management Committee	**Date approved:**	February 2020
Date reviewed:	March 2024	**Next review due by:**	March 2026
Policy Lead:	Nadine Gooding-Hebert	**Ownership:**	Cambridgeshire County Council

Type of document:	Policy
Document produced by:	Ben Stevenson, Data Protection Officer, Peterborough City Council Dan Horrex, Data Protection Officer, Cambridgeshire County Council
Document approved by:	Cambridgeshire & Peterborough Information Management Board,
Version :	Version 1
Issue date:	February 2020
How is this shared?	Email
Date due for review:	Annually April
Reviewer:	Ben Stevenson, Data Protection Officer, Peterborough City Council Dan Horrex, Data Protection Officer, Cambridgeshire County Council

Information Governance contacts		
Contact Details	**Email**	**Phone**
Cambridgeshire County Council	data.protection@cambridgeshire.gov.uk	01223 699137
Peterborough City Council	dataprotectionofficer@peterborough.gov.uk	01733 45387/452533

"If you only read this page then…."

Do ask for only the information you need to do the job and only keep it for as long as you need to

Do be clear about why you are collecting the data

Do only use information for the reason it was collected and seek advice if you need to use it for something else

Do dispose of paper records and emails securely

Do use strong passwords to protect devices and data

Do use secure and encrypted devices

Do make sure you know who you are talking to and check their identity if you need to

Do check someone's email or postal address before you send anything and make sure you always update records to make sure they are accurate

Do check what is in an envelope or email before you send

Do use the report if any data is lost/misplace/misused, for advice or if someone asks to see information held about them or wants their information deleted

Don't share personal information unless you are sure you can and you know who is asking

Don't assume that someone's consent last forever and covers everything

Don't leave PCs, laptops and phones unlocked or share your passwords

Don't leave personal information on show on desks or in vehicles - make sure it's secure

Don't open emails or click on links if you don't recognise the sender - speak to ICT

Don't write comments about an individual that we cannot defend - they have a right to see them

Don't ignore a possible data breach - the sooner it is reported, the sooner it can be dealt with

Don't think data protection does not matter, it does!

Introduction

We need to collect and use different types of information about people that we provide services for and communicate with in order to deliver those services. These could include children, vulnerable adults, current, past and prospective employees, contractors, suppliers, service users and carers.

In addition, we may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data.

The General Data Protection Regulation 2016 and Data Protection Act 2018 are pieces of law which will call data protection legislation. These explain the requirements and safeguards which we must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised.

Data protection means when we record and use personal information then we must be open about how the information is used and keep it secure. It applies to how we collect, use, shared, keep, delete and destroy personal information. s we use and decide how we use personal information, we have to ensure we comply with data protection legislation.

This policy applies to all personal data held by or on our behalf. It includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Why do we have a policy?

The purpose of this policy is to make sure that we:

· Comply with the law in respect of the data we holds about people

· Protect our customers, service users, employees and other individuals

· Protect the organisation when a data breach happens

· Follow good practice

We recognise we have a responsibility to make sure we comply with all of our data protection duties. We also have to ensure that all of our employees and suppliers not only understand but comply with data protection legislation.

Who does the policy cover?

This policy applies to anyone accessing or using personal information, including for example: employees, temporary or contract staff, volunteers, work placements, contractors, suppliers, services providers or other partners or agencies.

We have to make sure that anyone delivering a service on our behalf complies with this policy and others to make sure our data is safe.

What are our responsibilities?

There are six Data Protection Principles with which we must comply with in relation to personal information. In summary these are that personal information will be:-

1. Processed fairly and lawfully in a transparent way

2. Obtained only for one or more specified and lawful purposes and not further processed in a manner incompatible with that purpose

3. Adequate, relevant and limited to what is necessary

4. Accurate and where necessary, kept up to date

5. Not be kept for longer than is necessary

6. Protected by appropriate technical and organisational measures

This means that we will:-

· Make sure that when we ask for information then we are fair to the people whose information we ask for and use

· Explain why we are asking for the information and what we will do with it

· Make sure we only ask for the information we need

· Make sure the information we hold is up to date and accurate

· Make sure we only keep it for as long as we need to

· Ensure that we have processes in place to protect the information whether it is on paper or electronic.

· Ensure that we won't send information abroad unless there are the proper safeguards

· Make sure that people can exercise their data protection rights

In addition we will also:-

· Have someone with specific responsibility for data protection

· Make sure all employees know that they are responsible for data protection and know what good practice is

· Train staff to manage and handling information correctly

· Support staff to manage and handle personal information correctly

· Respond to any queries about handling personal information promptly and courteously

· Review how we use personal information to make sure we are always complying

· Ensure staff know when they can share information with others

What are your responsibilities?

All of us, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to the personal data that we may handle in the course of our work.

All of us must:

· Understand the main points of the Data Protection legislation

· Identify and report any risks their line manager

· Make sure that customers understand their rights

· Identify any breaches or loss of data and report them

· Identify and report any rights requests to the Data Protection Officer and their team

People have rights

Data protection legislation has introduced a set of rights for people. These are explained below and how we meet these.

The Right to be Informed

This means that people have a right to be told what we are doing with their information. We need to be clear and transparent about what we do because this helps build understanding and trust about what we do.

The way we normally tell people about what we do is in what we call a privacy notice. Our privacy notices will normally be available on our website so that people can easily find them. You can find out more in Made Simple #1: Peoples Rights.

The Right of Access

If we hold information about a person then they have a right to see their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them. We may have to redact some of the information if we cannot share something with a person. Information on redaction can be found in our IG Made Simple #1: People's Rights.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team and then it can be dealt with in accordance with our Subject Access Process.

The Right of Rectification

If we have some information about someone which is inaccurate or not complete then they can ask to amend or rectify it.

We have to respond with a month.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights..

The Right to Erasure

This is popularly known as the "right to be forgotten". It means that people can ask us to delete or remove information if there no strong reason for us to keep it.

We don't have delete information. The below table indicates when we may agree to delete and when we will not

To delete…	Or not to delete…
We no longer need the information	to exercise the right of freedom of expression and information
We should not have the information	We need to keep it to comply with a legal obligation
Our customer withdraws their consent	We need to keep for public health purposes
Legally we should have deleted it	It is of public interest for scientific/historical research or statistical purposes
Our customers objects to what we are doing and we cannot justify keeping the information	We need to keep it for the defence of legal claims

We always need to listen and understand why someone asking us to delete. We may have to keep some information, for example it is about safeguarding or health and safety. We should still take into account the customer's concerns and look what we can do to help reduce any distress or concerns they may have.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team. and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights..

The Right to Restrict Processing

A person has the right to block or suppress the use of their information. If someone does ask us to restrict the use of their information then it means that we can retain the information but not use it any further.

We will need to keep some information to ensure that we maintain the restriction.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights.

The Right to Data Portability

This is a right which allows people to obtain and reuse their data for their own purposes. It allows them to move, copy or transfer personal data from one IT system to another securely.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team. and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights. The Right to Object

An individual can object to what we are doing with their data where if it is based on:

· our legitimate interests or

· public interest or statutory duty or

· direct marketing or

· purposes of scientific/historical research and statistics.

The objection must relate to the person's particular situation.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights.

Rights related to automated decision making including profiling

A person has the right to not be the subject of a decision if it is based on automated processing and it produces a legal effect or significant effect on them.

The right does not apply where processing is necessary for the performance of a contract, authorised by law (including fraud) or there is explicit consent.

Applications can be made via our application form on the website, or our online form or making contact with the relevant team, either PCC Information Governance team or CCC Information Governance team. If you receive a request then please refer it to the relevant team, either PCC Information Governance team or CCC Information Governance team and then it can be dealt with in accordance with our IG Made Simple #1: People's Rights.

NHS National Data Opt Out

In addition to the rights under data protection, people have another choice when it comes to health records which contain a type of data called confidential patient information. This data can be used to help with research and planning. Patients can choose to stop their confidential patient information being used for research and planning. The choice will apply to the health and care system in England. They can do so by making their choice here

If you choose to stop your confidential patient information being used for research and planning, your data might still be used in some situations such as:

· When required by law – if there's a legal requirement to provide it, such as a court order.

· When you have given consent - if you have given your consent, such as for a medical research study.

· When there is an overriding public interest - in an emergency or in a situation when the safety of others is most important. For example, to help manage contagious diseases like meningitis and stop them spreading.

· When information that can identify you is removed - information about your health care or treatment might still be used in research and planning if the information that can identify you is removed first.

· When there is a specific exclusion - your confidential patient information can still be used in a small number of situations. For example, for official national statistics like a population census.

Services should ensure that they have a process for responding to notifications or requests relating to this. You should seek advice from the relevant IG contact to assist if needed.

What does 'it' mean?

Personal Information

Personal information is information about a living individual who you can identify directly or indirectly from that information. It may also be possible to identify an individual from that and other information which is in the possession of, or likely to come into our possession. It also includes any expression of opinion about the individual and any indication of our intentions.
It is also important to note that information to identify a living person is not limited to names and full addresses. Mapping point data can also potentially identify a person as can limiting the address to postcode.

Special Categories of Personal Information

Special categories of personal data, formerly known as sensitive personal data, means personal data consisting of information as to -

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union
- genetics
- biometrics
- his/her physical or mental health or condition,
- his/her sexual life,
- sexual orientation

In addition, we would consider the following to be sensitive:

- the commission or alleged commission by him/her of any offence,
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
- Credit card/debit card details pertaining to the data subject

Data Controller

The Councils are data controllers and will be responsible for ensuring compliance with data protection legislation. It means, on some occasions, that we determine what data is collected and how it is used. Where someone acts completely on behalf of a Council then we are still the data controller.
You should refer to the contract for providing a service to understand who the data controller is.

Joint Data Controller

There will be occasions where two or more controllers jointly determine what information is collected and why. This could be CCC and PCC or NHS. We need to make sure that customers understand when this is the case.
You should refer to the contract for providing a service to understand when joint controllers exist.

Data Processor

A data processor is the person/service who use the information as per the controller's instructions. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where permitted. Any use or sharing of data should not be done without the written consent of the data controller.
You should refer to the contract for providing a service to understand who the data processor is.

Data Controller-Data Processor Relationship - Contracts

Where the controller and processor are not the same i.e. the council and NHS, the relationship must be underpinned by a contract.
It is very important that we have a contract in place for us to deliver services or for something to be done our behalf. The contract has a really important role to play because it makes sure that all concerned understand what should be delivered.
Any contract must contain detailed schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. In all cases, Legal will review every contract and ensure that it meets requirements. The contract between the councils and suppliers will make clear that the liabilities and duties of data protection legislation which must be complied with
These kind of terms will be defined in the contract.

Advice on the process for buying and providing services can be found IG Made Simple #7: Procurement & Contracts.

When data is lost or goes missing…

We hold information which can be personal and sensitive information but also, for example, commercially sensitive information or simply data.
We have to take every care to avoid a data breach by protecting personal information and also by taking steps to avoid losing any data.
In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. IG Made Simple #2: Data Breach? covers the process.
You should report any breaches, suspected and confirmed, to the relevant team, either PCC Information Governance team or CCC Information Governance team. Guidance can be found the process in the IG Made Simple #2: Data Breach?

Keeping Information

We have to keep information but only for as long as we need to.
We will store personal information securely in our IT systems or in hard copy in line with our retention schedule.
We will destroy personal information securely by using confidential waste bins.
More can be found IG Made Simple #5: Keeping Information.

How we handle information

Whenever we handle information then we should do so securely. This should mean that we store is securely in systems protected by usernames and passwords or filing cabinets that are locked. It also means making sure that only people who should see that information have access. When we share or send information then we should make sure that it is secure. More information can be found in IG Made Simple #9: Safe and Secure Emailing.
The sharing of personal information must be by secure means such as secure email or secure file sharing may also be used after review by IT and in line with our ICT policy. Failure to comply with this policy will result in the appropriate action being taken under either the relevant policy or contract.

The Sharing of Personal Information

We will only share personal information where a legal gateway exists or consent has been obtained.
Sharing means telling someone some information about them or another person and sharing means giving a supplier a list of people.
You should make sure you know whether you should share and consult your Data Protection Officer, PCC or CCC, if you are not sure.
We should not use personal information to plan of service provision.
Please see IG Made Simple #4: Sharing Safely.

Disclosures permitted by law

There will be occasions where the disclosure of personal information will be permitted in law such as for the prevention and detection of crime or safeguarding of vulnerable individuals. We will always seek a written request confirming the reason for the disclosure where consent has not been obtained and will evaluate that request before responding. Equally we need to make our own requests in a lawful and proper way. You should look at IG Made Simple #8: Can it be disclosed? to help you with this.

Information sharing agreements

Any sharing of personal information between organisations may be best supported by an agreement that makes clear what is being shared, why and how. It helps us ensure we are complying with data protection legislation.

Further guidance on the completion of Information Sharing Agreements is contained within the IG Made Simple #4: Sharing Safely or can be obtained from the Information Governance service.

Should you enter into an information sharing agreement, you must provide a copy of the agreement to the Information Governance service prior to the information being shared.

Testing of systems

We may need to test that computer systems developed to bring greater efficiency, benefits and security work appropriately. In order to do so then we will need to consider using personal data in that testing. The first consideration will always be whether personal data is required for testing and the default will be that it is not with anonymised or randomly generated data being used. However this may not fully test the functionality of a system, therefore consideration must be given to the use of a data snapshot from the live or current system.

We will undertake a data protection impact assessment prior to the use of any current or identifiable data to ensure that this is appropriate and that the appropriate safeguards are in place prior to the export, import and testing. The data will only be held in the test system for the period of testing and then removed. If the testing of the system is being undertaken by a partner or a processor then the same process will apply.

Privacy and the value of information

Data protection is all about privacy. When we use information about people then we have an impact on their privacy in some way.

This could be when we think about buying a new IT system or running a new project or service. It means we need to think about the impact on our customers; how will it affect them? Will it make a change on their lives? Are there any risks that we need to think about? The changes in data protection in 2018 made it mandatory that we have to consider the impact and show that we have.

IG Made Simple #3: A DPIA Matters provides guidance on this.

Data Protection Impact Assessments (DPIA)

There are two levels of a DPIA; the screening process to work out whether you do need to do a DPIA is the starting point. This should always be completed whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals.

The completed screening checklist should be shared with the Data Protection Officer to determine whether any further assessment is required. They will inform you as to whether a DPIA is needed.

These can be published so it is important to make sure we have assessed impact and risk.

Only use what you need to use

It can be helpful to think about what level of information you need to use. Do you need to use every bit of information we hold about a person? Can you limit what you do use? You may only need ages and post code for example rather than their name, address, date of birth, NI number, health details and ethnicity. There are other ways of using personal information without sharing who that person is.

Anonymisation of data

Data can be anonymised i.e. removal of information which could lead to the identification of an individual. It should be almost statistical because there should be no way that you can identify any individual person. It is not enough to remove the name and address.

Pseudonymisation

Where it is not necessary to share personal data but anonymised is not sufficient, then consideration should be given to the pseudonymising approach. This means when information is supplied it is not identifiable to the user but the individual producing the information has a "key" to identify.

Information as an asset

When information is organised, stored, used and analysed then it is an asset that we can use. This means that we need to make sure it is managed properly. This management means that we know what we hold, where it is held, how long for and its qualities. This will help us use the information we have much more efficiently and better because we will understand it more.
Each service will have an Information Asset Owner (IAO) who is responsible for understanding that information, making sure it is only disclosed appropriately and is securely held.
More information can be found in IG Made Simple #6: Information is an Asset.

Roles

Chief Executive

The Chief Executive has overall accountability and responsibility for data protection. The Chief Executive is required to provide assurance that all risks to ADS relating to data protection and information security are effectively managed and mitigated.
The Chief Executive has delegated responsibility for compliance with the Data Protection Act (including the implementation of this policy and other related policies) to the Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

Sue Grace, Director of Customer and Digital Services is the SIRO for CCC and Fiona McMillan, Director of Law & Governance and the Monitoring Officer is the SIRO for PCC. They are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Overall ownership of the CCC & PCC Information Management policies
- Act as the champion for IMAG at the councils and on the Information Management Board and provide written advice to the Accounting Officer on the status of IG and IM within CCC
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls
- Owning the organisation's information incident management framework
- Ensuring that they receive appropriate training to fulfil the SIRO role.
-

Data Protection Officer

The Data Protection Officers, Dan Horrex (CCC) and Ben Stevenson (PCC) will:

- Manage the compliance with data protection legislation and FOIA
- Maintain an awareness of all IG/IM issues within CCC & PCC respectively
- Review and update the IMAG in line with local and national and best practice requirements

- Review and audit all processes and procedures relating to IMAG where appropriate and on an ad-hoc basis
- Ensure all line managers and staff are aware of the requirements of these policies and guides
- Set a list of minimum expectations for security standards for IT systems.

Caldicott Guardian

Helen Duncan (Adults Services) and Anna Cullen (Children's Services) have been appointed Caldicott Guardians for their respective areas and will:

- Ensure that CCC & PCC satisfies the highest practical standards for handling patient identifiable data;
- Facilitate and enable appropriate information sharing and make decisions on behalf of CCC & PCC following advice on options for lawful and ethical processing of information, particular in relation to disclosures;
- Represent and champion relevant IG requirements applicable to the role at Board level;
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within and outside CCC & PCC.

Cambridgeshire & Peterborough Information Management Board

The Councils' have a shared board chaired by the SIRO and attended by representatives of all directorates. This is a key board to determining strategy and having oversight of all things data protection.

Responsibilities of Managers

All managers are required to ensure that they and their staff understand this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy.
All managers must identify and report any risks or breaches to the relevant team, either PCC Information Governance team or CCC Information Governance team.
All managers must ensure that their staff undertake data protection training refresher training which will be undertaken annually.

Additional responsibilities for Managers - Temporary Staff

It is a requirement of Peterborough City Council that all temporary staff, agency staff, volunteers, work placement students and all managers requesting access to systems for these temporary workers, should read, and undertake to comply with these compliance guidelines. Managers should ensure that any such staff are trained and understand data protection responsibilities.

Responsibilities of Members

All elected Members have responsibilities in their own right and when considering the use of personal information for any particular purpose, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.
Members should also refer to council's "Members' Code of Conduct", which is intended to promote high standards of behaviour amongst the elected and co-opted members of the council and which is available on the council's website.