Freedom of information request for information relating to the use of payment cards

Name of your Local Authority

- Nottinghamshire County Council

1. **Who is the data controller for personal data relating to payment cards?**

- PFS is the Data Controller, the Council is the Data Processor

- **If it is the card provider, is there a contract in place covering this data processing?**

- Yes – NEPO framework agreement

2. **Who has access to the data?**

- Direct Payment Quality Officers
- Business Support Officer
- Client finance team leader
- Client Finance officers
- Children's and & Families Dept commissioners
- Adult Client Finance Services (ACFS) Direct Payment auditors
- Adult Client Finance Services Team Leader
- PFS (card provider) staff

- **What data protection training have these staff had?**

- GDPR training – mandatory for Council staff

- **What organisational measures – policies and procedures are in place to ensure that data is kept safe and not accessed by anyone without authorization?**

  GDPR Policy and associated staff guidance
  Corporate privacy statement
  DP specific privacy statement
  ACFS DPIA (still in draft – pending final sign off)

Response from PFS:
All access to systems and data is based on the ISO27001:2013 'least privilege-based access' permissions. Managers are responsible for approving minimum access required for members of staff to successfully complete their role. All accounts and actions are fully auditable with staff being accountable for each action taken.
Only staff with permission to access the data are allowed, with the exception of a limited number of administrators, whose own access is logged and monitored by the Information Security Manager.

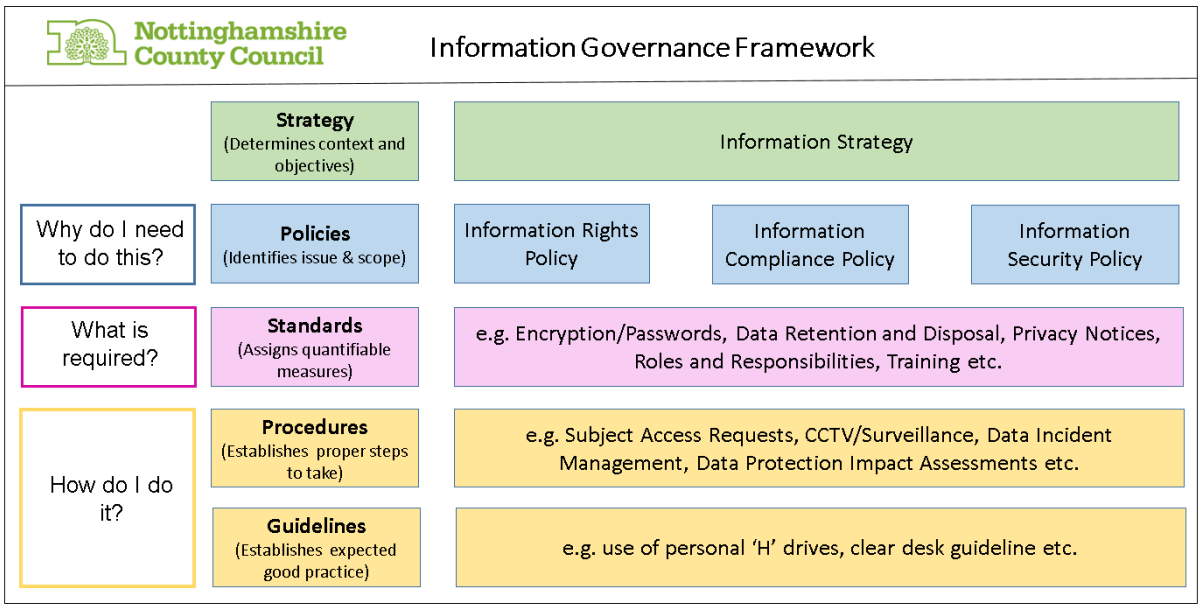
Each member of staff is issued with a unique ID and P/W with strictly enforced password strength and duration.
All PFS staff undergo Employee training (mandated policy) which goes through a number of different aspects of the business and includes a section on Data Protection, the importance of handling such data, issues that may arise and how to handle different enquiries. All line managers have the responsibility of ensuring that their department staff are well informed of their responsibilities.
All PFS staff complete a 'new' IT Security and Compliance training 'every 4 weeks', among others, this includes Data Loss Prevention, Information & Data, Data Classification, GDPR and PCI.
Several policies are in place, including IT Security Policy, Data Classification Policy, Password Policy, Secure Media Policy, Privacy Policy, Data Protection Policy, Data Retention Policy which all provide measures to ensure data is secure and not accessed by non-approved personnel. Policies and Procedures have a data classification of 'Internal', so cannot be shared outside of the Company.

- **Please provide a copy of any written policies and procedures.**

The key policies are the:

- **Information Rights Policy** – aimed at the public
- **Information Compliance Policy** – aimed at all staff
- **Information Security Policy** – aimed at staff and ICT specialist staff

These policies are supported by standards, procedures and guidelines which are shown in the framework diagram below.



ASCH Direct Payment Policy - Link

3. Have payment card users been asked to sign a privacy notice?

- DP Agreement links to DP privacy statement and corporate Privacy Statement

- **What formats is the privacy notice available in?**

- Electronic format and hard copy can be requested by calling NCC customer contact centre. Customers who phone the customer contact centre also have the option to listen to an audio recording containing privacy information.

- **Please provide a copy of the privacy notice:**

NCC Privacy statement - Link
ASCH Direct Payment Privacy statement - Link

Response from PFS:
Please find our Privacy Policy on the below website:
https://prepaidfinancialservices.com/en/
under section:
https://prepaidfinancialservices.com/en/privacy-policy

4. **What steps have been taken to keep payment card data secure? payments?**

- All personal data is kept within a secure multi encrypted online portal operated by PFS (card provider).
- ACFS files kept in secure NCC digital files with restricted access.

Response from PFS:
Being PCI DSS level 1 compliant, we carry out regular Firewall rule reviews, have Intrusion Detection / Prevention protection, best in class Web Application Firewalls, DDoS infrastructure protection, File Integrity Monitoring, active threat hunting, internal and external vulnerability scanning, supported by both a Crisis Management & IT Security Incident Management Process/Procedure.
As an FCA regulated and PCI DSS certified corporation, the PFS Rackspace environment meets numerous certifications such as PCI DSS, ISO27001:2013, ISO 9001:2008, ISO14001:2004, PCI DSS, Cyber Essentials Plus, SOC1/2. This means independent verification has taken place to evidence resilience, redundancy, power and generator testing at least annually to ensure backup services and providers meet and/or exceed the PFS contractual expectations.

- **What protections are in place to guard against fraud?**

- The PFS portal needs Service Users to verify their identify via a password and the website has to verify identity with secondary personal information.

- **How is the cardholder's information (including information as to the account holder as well as any purchases) stored?**

- PFS portal and ACFS system

Response from PFS:
Where appropriate cryptographic controls will be used to protect the confidentiality, authenticity or integrity of information that is considered at risk.

As a data controller, PFS ensure the confidentiality and integrity of data-at-rest is maintained due to multiple encryption algorithms and mechanisms that are employed on the basis of security standards recommended by the PCI DSS security council and NIST and SANS Institute. This encryption is also on all data backups.
Fraud enabled defences include monitoring of unusual spikes in activity, reputation and cyber threat intelligence supported by a dedicated and proactive Fraud team.
PFS also meets the requirement for secure data storage by ensure it is physically secure, and it is processed by and stored within the service and the legal jurisdictions of the UK. Our data is currently stored in a Rackspace PCI DSS accredited data centres, on physical & virtual servers, in 2 locations (both in the UK). The data is held in its own private room, with specific access rights and controls and we operate a full data recovery and backup policy.

• Equipment is protected from power failures and other disruptions caused by failures in supporting utilities and dedicated independent generators are in place.

For other electronic information held on computers /servers is it backed up on a daily basis. All data is stored on servers offsite within the Rackspace data centre which is backed up and provide a back-up system should the operating servers go down.
PFS has a robust shredder located in the office which allows for the safe and secure disposal of any information that is held on paper. No information is held on DVDs.

- **What technical and organisational measures are in place in respect of the payment card platforms and any associated network and information systems, e.g. to prevent cyber attacks?**

- NCC have many technical and organisational measures in place to prevent cyber attacks and to protect networks and information systems. These include multi-tiered next generation firewalls, intrusion detection and industry leading endpoint detection and response clients on all devices. There is also a suite of information security policies and associated processes, covering a variety of security controls including vulnerability management, passwords, access controls and encryption. The security of these technical and organisational controls is independently verified as part of our Public Services Network compliance and our Cyber Essentials certification, each of which requires an annual independent penetration test.

Response from PFS:
Being PCI DSS level 1 compliant, we carry out regular Firewall rule reviews, have IDS/IPS protection, best in class Web Application Firewalls, DDoS infrastructure protection, File Integrity Monitoring, active threat hunting, internal and external vulnerability scanning, supported by both a Crisis Management & IT Security Incident Management Process, Procedure. PFS maintains full intrusion and antivirus software on its systems. We run quarterly internal and external vulnerability scans and at least an annual independent penetration test, together with our disaster recovery and anti-virus protection systems have to be audited every year by MasterCard.
PFS are PCI DSS Level 1 certified which means numerous Policies, Standards, Procedures, Tools, Controls, Resources must all be in place and independently verified. PFS also have Cyber Essentials certification, the Data Centre is also ISO/27001:2013, SOC1/2, OHSAS 18001:2007, ISO 9001:2015, ISO 14001:2015 certified.
There are numerous IT Security controls in place at the perimeter, down to the endpoints (Laptops/PC's), using a 7-layer robust Security strength in depth approach. A high-level view of the framework can be found below showing some of the additional Security controls and policies in place.

- **What action is taken in the event of a data breach?**

- It would be reported directly to the Council's Information Governance Team who would report to ICO if required.
- This is underpinned by a Security Incident Response Standard (http://home.nottscc.gov.uk/working/ict/security/policies/incident-response) and associated procedures.

Response from PFS:
In addition to our GDPR responsibilities to the FCA, PFS have a Crisis Management & IT Security Incident Management Policy/Process. Together this is used to ensure the right committee members are put together in a timely manner to determine short/long term risk effects and consequences of the data breach, work with internal, external partners/clients, agencies, including the police and media if necessary. Clients are kept informed via their regular Account Management team.
If a data breach is reported, PFS will report this to the relevant supervisory authority (Company DPO) and FCA within 72 hours of the organisation becoming aware of it. In addition, PFS has an internal Disciplinary Procedures Process which sets out the policies and processes for dealing with any disciplinary offences by employees. A forensic root cause investigation will commence and any areas of procedures that can be improved are documented and re-issued to staff together with further training as required.

- **What arrangements are in place to enable access to funds in the event of a system failure?**

Response from PFS:
In addition to live production services, PFS take pride in our high-level system uptime and comprehensive business continuity planning processes. We have a resilient live service with quick failover in the event of system failure. In addition, PFS have a Disaster recovery plan/process which includes physical backup systems replicated in a 2nd UK based data centre. This includes different utility and service providers allowing PFS to ensure quick recovery in the event of complete system failure.

5. **Have you carried out a Data Protection Impact Assessment?**
   - NCC has not completed a DPIA relating to the use of Pre-paid debit cards.

Response from PFS:
Yes - Each Department Head is responsible for monitoring the performance of the individuals in their department and for keeping them informed of any developments relating to Data Protection. Each Department head also is responsible for monitoring the performance of individuals.
In our call centre, calls are recorded for monitoring and training purposes and a random selection of calls are reviewed on a monthly basis to ensure compliance with all our policies including data protection. This also applies to e-mails.

- **What risks have you identified? And what mitigating action are you taking?**

Response from PFS:
A breach is reported to the relevant supervisory authority (Company DPO) within 72 hours of an organisation becoming aware of it. Depending on the scale of the breach, it may be impossible to investigate a breach fully within the given timeframe, so organisations will be allowed to provide information in phases. Any identified risks are added to the Company risk register which is reviewed by the Board of Directors on a quarterly basis.

- **If you have identified any high-level risks that you are unable to mitigate what action are you taking as a result?**

Response from PFS:
Departmental risks are regularly reviewed with high risk items aggregated up to the Board of Directors who review quarterly. There are currently no high-level risks that do not have mitigating controls in place.

6. **What processing operations do you actually carry out on the personal data collected?**

Response from PFS:
PFS is a Data Controller under this structure

- **Who reviews the data and how often?**

Response from PFS:
Any member of staff whose access has been approved by Management may review this on a daily basis. Security application logical access reviews take place to ensure only approved accounts can access systems with account re-certification regularly taking place. Changes to permissions/applications can only be approved by line Manager and logged in an industry leading Incident and Change management tracking system.

- **Are reviews ad hoc or routine?**

Response from PFS:
Reviews are both routine, and Ad Hoc. Our robust security defences provide Clustered Firewalls, Web Application Firewall's, Intrusion Detection/Prevention systems in place at the perimeter to ensure only approved transactions/devices can access the PFS data. Quarterly reviews are/will be completed to validate access rules, device firmware and policies to prevent all unauthorised access.

- **If ad hoc, what triggers a review.**

Response from PFS:
PFS can, and will, call Ad Hoc reviews where unforeseen events arise, which PFS believe require an urgent review of the circumstances surrounding the event to be reviewed, in detail.

- **Are card holders notified of a review?**

Response from PFS:
Where PFS deem that a real risk to the card holders security exists, PFS will notify card holders of such review being performed.

7. Which organisations, if any, is this data shared with?

Response from PFS:

Sub-Supplier details: (name, address and company registration number)	Nature of sub-processing:	Commencement date of contract between Supplier and Sub-processor:
Rackspace Unit 8 Unit 8, Millington Road, Hayes, Middlesex, England, UB3 4AZ Company number: **03897010**	Managed/Hosting	Commencement (and Renewal) – 25th January 2018.
M2 3000 Hillswood Drive, Hillswood Business Park, Chertsey, KT16 0RS - 500 Winderley Place, Suite 226 Maitland, FL 32751	Processor	Commencement (and Renewal) – 1st July 2016.
Gemalto Concorde Way, Segensworth North, Fareham, Hampshire, PO15 5RX Company number: **01278148**	Card Vendor	Commencement (and Renewal) – 13th July 2016.
eComm Merchant Services IDA Business & Technology Park, Johnstown, Navan, County Meath, C15 E8KV, Ireland Company Number: 540660	Acquirer	Commencement (and Renewal) – 4th June 2014.

- **Have you drawn up an Information Sharing Agreement (ISA) to govern this sharing activity?**

Response from PFS:
Yes, there is Data Protection Agreement in place between the Council and PFS, which adheres to the GDPR.