

Information Exchange Protocol
agreement between
DUNDEE CITY COUNCIL - National Entitlement Card Programme Office
acting on behalf of Scottish Local Authorities as listed at Appendix C
and
IMPROVEMENT SERVICE acting on behalf of Scottish Local Authorities as
listed at Appendix C
For the sharing of data required to carry out data processing related to the
National Entitlement Card.

This Information Exchange Protocol (the “Protocol”) is between:

- (A) Dundee City Council of 21 City Square, Dundee DD1 3BY (“DCC”) acting on behalf of Scottish Local Authorities as listed at Appendix C;
- and
- (B) Improvement Service (“IS”) (a company limited by guarantee incorporated in Scotland with company number SC287978 whose registered office is c/o CMS Cameron McKenna LLP, Saltire Court, 20 Castle Terrace, Edinburgh, EH1 2EN) acting on behalf of Scottish Local Authorities as listed at Appendix C.

For the purposes of this Agreement the “Partners” means Dundee City Council (acting on behalf of Scottish Local Authorities) and Improvement Service (acting on behalf of Scottish Local Authorities).

Dundee City Council and Improvement Service shall ensure that all Scottish Local Authorities are provided with a copy of this Protocol and are aware of their duties and obligations arising from this Protocol.

1. PURPOSE AND LEGITIMATE AIM

- a. The purpose of the Protocol is to facilitate the exchange of information between the Partners that will enable them to carry out data processing related to the National Entitlement Card (NEC) scheme (“the Scheme”). The Scheme is the shared smartcard platform adopted by Scottish Local Authorities and other parts of the Scottish public sector to deliver customer-centric services including national concessionary travel entitlements and smart transport ticketing as part of the Customer First programme.
- b. Dundee City Council are data processors making use of the Card Management System (CMS), the associated NEC Online functionality and associated card production services to allow the Scheme to manage and produce cards.
- c. Improvement Service are data processors making use of the myaccount system to offer data verification, notification and online authentication services to the Scheme.
- d. In order to manage the personalised smartcard scheme, it is necessary to collect and process Personal Data and so the provisions of the Data Protection Act 1998 (“DPA”) are applicable.
- e. Individual Scottish Local Authorities are the designated Data Controllers for the data collected and maintained to issue NECs and manage the Scheme. Local Authorities make use of services provided by Dundee City Council and Improvement Service to process this data on their behalf, and the Partners are required to exchange information as a result.
- f. The Protocol is underpinned by other Agreements that govern or state the nature of Data Sharing and Data Processing that takes place. These agreements are listed at Appendix A.

2. APPLICATION

a. The Partners subscribe to the following for this Protocol and any sub-Protocols:

i. The agreed standards must provide safeguards and an appropriate framework for the controlled exchange of relevant information as outlined below.

ii. The principles of the Data Protection Act 1998 must be upheld. (See The Data Protection Act 1998 Principles 1-8).

iii. All Partners must be compliant with the Human Rights Act 1998.

iv. The Partners will periodically review this Protocol. The first review will be within 6 months of signing, thereafter annually. However intermediate and subsequent reviews may be initiated by any changes in legislation, case stated or ruling by the Information Commissioner.

v. Partners may request changes to this Protocol at any time by submitting a suggested revision to the Protocol holder in writing. Any suggested alterations to this will be discussed at the next NEC Board meeting at which both Partners are represented. All decisions must be minuted and their actions recorded and retained by the protocol holder.

b. The nominated holder of this Protocol is the Authorised Person at Dundee City Council, who shall, on behalf of the Partners:

i. Ensure that a review is carried out in the first six months of the document being signed and then subsequently reviewed on an annual basis.

ii. Circulate all requests for change, co-ordinate responses, obtain agreement for the changes from the Partners.

iii. Appendix B contains a list of Authorised Persons that should be referred to in each organisation.

3. NOTIFICATION

a. For the purposes of the DPA, Local Authorities are required to be registered as Data Controllers in order to provide data to either of the Partners for processing.

b. Their registration should cover the appropriate criteria for processing from Schedules 2 and 3 of the Data Protection Act 1998.

4. CONDITIONS FOR PROCESSING

a. As part of the process of accepting applications for National Entitlement Cards, Local Authorities inform prospective cardholders that the data they provide will be shared with other Partners to the extent required to administer the Scheme, and applicants are required to give their consent to this in accordance with condition 1 of Schedule 2 of the DPA.

b. Certain prospective cardholders may have also consented to additional sharing of data, but the sharing of data under this Protocol does not depend on that consent, which itself does not form part of the data exchanged.

5. DATA EXCHANGED

a. Daily File data. The data identified in the Daily File specification (Annex III) is exchanged between the myaccount (IS) system and the CMS (DCC) in two ways:

- i. Data is exchanged between myaccount (IS) and CMS (DCC) on a daily basis as per the specification in order to allow
- A) subsequent or continued secure online access to NEC Online by Customer utilising myaccount;
 - B) receipt within CMS of definitive address reference and potentially format from One Scotland Gazetteer on the basis of Customer supplied data;
 - C) receipt within CMS of UCRN under the related Agreement between NRS and the LA (see Appendix A);

D) exchange of changes to personal and contact details recorded in either CMS or myaccount which may subsequently be applied in the other system.

ii. Data files are produced on an occasional ad hoc basis by both myaccount (IS) and CMS (DCC) systems, and passed to the other Partner to allow data integrity between the Partners to be confirmed or corrected.

b. SAML data. The data identified in the SAML specification (Annex I) is passed from IS to DCC in two ways:

i. During the process of a Customer using the IS myaccount (IS) system to access NEC Online (DCC), when a Customer successfully logs in to myaccount and consents to share data with NEC Online, the data in the specification is shared securely with NEC Online and hence with the CMS (DCC) to help ensure that the user is given access to the correct personal details.

ii. A myaccount (IS) report containing the SAML data relating to myaccount records where the Customer has consented to share data with the NEC Online (DCC) system is provided on a weekly basis to DCC. This is a short-term arrangement to assist in diagnosis of problems that Customers may report in using the NEC Online system with myaccount.

c. Support Request data (Annex II) is made available to NECPO (DCC) by IS when the support request relates to the NEC Scheme; this is to help provide a speedy resolution to Customer queries.

6. THIRD PARTIES

a. Acting on behalf of the Data Controllers, the Partners may appoint Third Parties to process data. It is imperative that should a partner be party to such an arrangement, that the processing is carried out with appropriate safeguards in place (see 10). Partners should therefore ensure that:

i. Contracts or agreements between themselves and external suppliers include adequate and concise requirements for the processing, security and exchange of personal data. The contracts/agreements must include the requirement for service providers to act only on instructions given by the partner.

ii. Guarantees are provided by the service provider in respect of security measures they intend to take, and partners should take reasonable steps to ensure the service provider complies with those measures.

iii. Flows of information are limited to those that the partner defines.

iv. Partners have sufficient access to confirm the adequacy of standards for the protection of data, to respond to any complaints and breaches, and also to satisfy data subject requests.

v. Partners carry out all relevant checks with prospective suppliers prior to awarding any contracts and refer back to the Data Controller prior to disclosure should their intention be to use the contractor to process or store shared data.

7. NOMINATION OF STAFF

a. To ensure compliance with the principle of security and the common law duty of confidentiality, this Protocol contains a list of appropriate nominated officers (see Appendix B - Authorised Persons) with whom contact should be made in relation to this Protocol.

8. ACCURACY OF DATA

a. There is a duty in the Data Protection Act 1998 on a Partner supplying personal data to advise the recipients of personal data shared if the data supplied is subsequently found to be inaccurate.

b. Where an inaccuracy is discovered after a disclosure has been made, it will be the responsibility of the Partner discovering the inaccuracy, to bring this to the notice of the data owner who should notify all recipients of the correction.

c. Corrections of this sort will normally be carried out on an ongoing basis using the Daily File mechanism mentioned below; however, occasional use will also be made of extract files with contents reflecting the data included within Daily Files to allow correction of inaccuracies that may have arisen.

9. RETENTION OF DATA

a. The Partners support the Data Protection Principle that data must not be retained for an excessive period. It follows that data must be destroyed as soon as it is no longer required for the original purpose for which it was supplied or collected.

10. SECURITY OF DATA

a. Each Partner must ensure they have appropriate security arrangements in place and take all reasonable steps to adequately protect the data from both a technological and physical point of view. This must include security of computer data, manual files and all forms of transfers of data between Partners.

b. In the event of a security incident resulting in the loss or potential loss of data whilst in the care of one of the Partners, the Partner's Authorised Person should ensure that the relevant parties, including the appropriate Data Controller, are advised.

11. DATA SUBJECT REQUESTS

a. Individuals have the right of access to a copy of all information held about them on computer and manual files - unless an exemption applies where information can be withheld under certain circumstances.

b. Partners will refer all those making data subject requests to the relevant Data Controller.

12. FREEDOM OF INFORMATION

a. The Partners shall co-operate in handling and disposing of any requests made to either of the Partners, under the Freedom of Information (Scotland) Act 2002 ('FOISA'), of the other. The Partners acknowledge that nothing in this Protocol is confidential.

b. Any requests received by either Partners under FOISA which relate to this Agreement shall be passed to the Authorised Persons for the Authorised Persons to decide which Partner should action and take overall responsibility for as soon as practicable after receipt and in any event within three working days of receiving the request.

13. COMPLAINTS

a. Any complaints will be brought to the attention of the nominated officer of the relevant Partner and will be dealt with in accordance with their organisations internal complaint procedures. In addition, the relevant Data Controller must be informed.

b. Partners and the relevant Data Controller will keep each other informed of developments following receipt of a complaint, where relevant.

14. CONFIDENTIALITY

a. Each Partner shall at all times keep confidential, all personal data supplied pursuant to this Protocol. This clause shall survive termination of the agreement or the withdrawal of or removal of any partner.

b. Any publication of data supplied pursuant to this agreement will not identify any individual.

15. COMPLIANCE AND GOOD PRACTICE

a. Any further guidance or codes of practice should be distributed via the Protocol holder for consideration and possible attachment to this Protocol.

16. CERTIFICATION

a. By signing this document the participants (identified below) accept and will adopt the statements included in it and agree to maintain the specified standards.

17. PUBLICATION

a. This Protocol is published by Dundee City Council on behalf of the Partners (as shown at the start of this Protocol). This Protocol can be made available to the public as required.

18. SIGNATORIES

By signing this Agreement Dundee City Council, acting on behalf of Scottish Local Authorities and Improvement Service, acting on behalf of Scottish Local Authorities, confirm that they accept its terms.

Dundee City Council

Signature Date

Paul Carroll, Transformation and Performance Manager
For and on behalf of Dundee City Council, acting on behalf of Scottish Local Authorities

Witness' signature

Witness' full name and address

.....

Date

Place.....

Improvement Service

Signature Date

Paul Dowie, Director, Shared Services & myaccount
For and on behalf of Improvement Service, acting on behalf of Scottish Local Authorities

Witness' signature

Witness' full name and address

.....

Date

Place.....