

Policy for Intellectual Property Rights and the Development of Software

Introduction.

This document describes the Nottinghamshire Police policy with regards the development of computer software and the ownership of any Intellectual property Rights to that software.

Nottinghamshire Police Preferred Options.

The core function of Nottinghamshire police is to provide a Policing and not to develop software. Therefore where there is an additional need to use software in the support of this core function the following questions need to be asked:

- Is there any existing software in use in force that is already suitable?
- Is there software available from established suppliers that is suitable?
- Is there any software available from other forces that is suitable?
- Could an external established supplier develop this software?

Only if the answer to each of these questions is “no” should the force consider the internal development of new software. No new in-house software should be commissioned without the agreement of force senior management, including the Director of Information & Network Services.

Software IPR

For all software used by the force on both LAN and standalone systems the ownership of the intellectual property rights of this software should be clear and unambiguous. This ownership could be registered with:

- A third party supplier (e.g. Microsoft)
- Nottinghamshire Police.
- Another Police Force (e.g. Leicester for Genie)
- A partner organisation. (GOEM)
- An individual.

The owner of the IPR of the software will then grant Nottinghamshire Police a licence for its use, which might be per user (e.g. Oracle), per computer (e.g. Microsoft Office) or force wide (e.g. ABM).

Software owned by Nottinghamshire Police will have universal usage rights (subject to security and technical restrictions) and can be licensed to other organisations subject to an external software supply policy (to be agreed). Responsibility for the support of software rests with the owner of the IPR. Where the IPR rests with Nottinghamshire Police then support rests with the Information and Network Services dept.

What is Software, what is data?

Clearly Microsoft Excel and the Fortek Polis system are easily distinguished as software. It is possible however to develop small software packages using desktop development tools such as Access. For guidance as to when Access should be used see appendix A. If the originator only uses these databases then they are not really classed as software anymore than an Excel spreadsheet is. If the database is used by several people and/or contains complex data and transactions then it should be classed as software, which then has an IPR and needs support. Any Access Database, Excel spreadsheet or Word document that contains automated routines; macros or visual basic code is software. By default if a file is not software it is data and subject to the Data Protection Act and Information Security Policy. The Chief Constable owns all Data held on force systems.

Software Register.

All software that has an IPR and therefore requires support is to be recorded on a software register. This register will contain details of the software; it's owner, function and licensing arrangements. The software register will be maintained by Administration(INS) under the responsibility of the Technical Manager INS (Systems & Databases). The suitable provision of support for all software will also be the responsibility of the Technical Manager (INS) who may arrange for support of certain specialist pieces of Nottinghamshire Police software (e.g. Merlin) to be undertaken outside of the INS department.

Ownership of Software by Individuals.

As a rule the use of software owned by individuals is not to be encouraged as it is unlikely that these individuals will have the resources to continue to develop the software or provide sufficient long-term support. Where there is a decision to use such software the supplier must provide a copy of the

software source that can then be used in the event of the individual no longer being able to support it. If the individual does not wish to provide this information directly to the force then they can use the NCC escrow facility on the basis that the cost of this is borne by the individual

Development of Software any members of the Force (Police and Civilian).

The following rules will apply to software developed by members of the force:

1. All software developed on force equipment becomes the property of the force.
2. All software developed during time for which the developer is paid by the force becomes the property of the force.
3. That the software may not be removed from force equipment onto private equipment nor may a copy of the software be removed from force premises without proper authorisation from the Information Security officer.
4. Software must only be developed when there is no other option. A full investigation of alternatives must always be undertaken including the use of existing systems, external packages and other force systems. If there is a clear requirement the first source of new software should be the INS department. Only if the INS department cannot either supply the necessary skills or outsource them should non-INS staff seek to develop software. In all cases the decision to develop new software must be signed off by the Director of INS.
5. In setting out to develop software the extent of the development should be set out at the outset. This needs to be documented as part of the overall business case for the development.
6. On completion of the Software full documentation is to be provided by the developer, in addition to a copy of the source code. The documentation should detail: the software's purpose; functionality; access levels; security elements such as password protocol and audit trail facilities; the language, including version, in which it is to be written; how it is to be structured and any other technical details that INS staff might need to maintain the application, rectify any problems or further develop the application.
7. No new software to be installed onto the LAN/WAN infrastructure without the approval of the Systems Support Manager (INS).

Current members of the force can retain the IPR of software if:

1. The software is developed wholly outside of their hours of work and on equipment owned by them or a third party.
2. The marketing of any software is wholly independent of their relationship with the force. The force's name cannot be used to create credibility.
3. No force resources have been used in the design or development of the software.

On retirement or leaving the force officers/employees may wish to develop software that relates to police specific applications. Where this is done then all code generated must be new. Use of existing force code will be considered a breach of copyright.

The Purchase of Software by the Force from serving officers/employees.

The force should not purchase software from serving officers or employees unless:

1. It is clear that the force has no rights to the IPR of the software. This can only be the case when the function of the software has previously been completely unrelated to the business of the force. If there is a potential claim and the member of the force has expended personal time in developing the software then compensation should be through either overtime or via an honorarium. Both of these payments will be subject to standard deductions for tax, N.I. and pensions.
2. That the additional hours worked in the production of this software have not led to the member of the force working outside of the Regulations and Agreements reached locally between the Chief Constable and Staff Associations.
3. The author can accommodate any necessary support arrangements in line with a service level agreement for the software without disrupting their normal duties. Support arrangements should also be put in place for when the author is away either on leave or on secondment.
4. A copy of the software is available in case of incapacity of the author. This copy to be free from passwords/encryption and lodged with HQ(INS) for security. Alternatively, an escrow arrangement with NCC will need to be paid for by the author (Current cost £400 initiation, then £250 per year)

5. Any data moving offsite to the author's premises must be subject to a Data Protection protocol and the premises subject to a security audit and compliance with the required ACPO security standard.

6. The software must be fit for purpose and suitable for operation within the force infrastructure.

7. The decision to purchase the software from the author has been made in accordance with Financial Regulations.

Protection of Third Party Intellectual Property Rights.

In the course of conducting business with third party software suppliers the force may have access to information that is commercially sensitive. This information may be of a technical nature and relate to designs or techniques to be used in a future development, or it may be information relating to future pricing. In some circumstances the force might be asked to sign a confidentiality agreement or be told that the information is "Commercial in Confidence". There may be other times that the information is given to us "in trust" that we would not pass it on to a potential competitor.

In these circumstances there is a potential conflict of interest if members of the force who gain access to this information in the course of their duties within the force may also find this information of value to the conduct of their own business.

Therefore it is proposed that in any discussions with third party suppliers members of the force should make known to the Director of INS any potential conflict of interest prior to meeting with third parties. The Director of INS will then ask the member of the force to remain at "arms length" from the discussions. Failure to declare such an interest where one exists will be referred to Professional Standards Unit.

Appendix A. Use of Access.

Access is Microsoft's small database application aimed at standalone PC's or very small network (2/3 PC's) with a fairly small database size and structure. Microsoft recommends that for anything over this level, more scaleable development tools (such as VB) and SQL server are used.

Therefore possible uses of Access within the Force could (although some are not recommended) be:

1) Single user database, where the database is stored on the user PC hard drive (ideal for standalone, but could also work on the LAN without INS backing up the data).

2) 2/3 User databases, where users are located in the same building and a NT server is present, the database and application can be held on a file share. Shared use of the Database over the WAN is not recommended.

3) 25/50 User database, but number of concurrent users is low, if users are located in the same building.

4) For large numbers of concurrent users we must follow Microsoft's recommendations and not use Access, but use other more suitable tools.

Note. Use of Citrix. It is possible to enable the use of Access across the WAN through the use of Thin Client or Citrix technology. This technique has been used with some success with the Magellan and Traffic Workbook software. It is however a complex solution that should only be applied to existing systems where redevelopment is not a feasible option.