BUSINESS, FINANCE AND DEMOCRACY
CABINET MEMBER MEETING
12 February 2014

ITEM 7

Derby City Council

Report of the Strategic Director of Resources

Information Security, Zero Tolerance on Compliance

SUMMARY

1.1 The report provides an overview on the stricter compliance regimes being imposed by various external bodies including the Cabinet Office and the Ministry of Justice and of the tougher penalties being imposed by the Information Commissioner's Office. Without additional and enhanced security we risk

- Being unable to process benefits or investigate fraud
- Being unable to comply with on line electoral registration requirements
- Failing a compliance audit leading to suspension of access to government data sets and/or to secure email
- Risk of enforcement action and possible fines by the Information Commissioner

RECOMMENDATION

2.1 To approve the implementation of the required additional and enhanced security measures detailed in Appendix 2 and now required in order to meet the Zero Tolerance approach imposed by the Cabinet Office.

2.2 To note that the requirements to impose new controls on baseline personnel security checks will be reported to the Personnel Committee.

2.3 To continue to use peer network s to lobby for a more practical and more affordable approach to security compliance.

REASONS FOR RECOMMENDATION

3.1 The Cabinet Office issued its Zero Tolerance Compliance Approach on 29 April 2013. We had achieved our compliance with the PSN network before this date and as such it first applies to Derby in February 2014. Failure to achieve a successful compliance certificate for the PSN network will mean that:

- Our access to the PSN network will be suspended
- We can no longer access government data required to process benefits and/or to investigate suspected fraud
- We can no longer access the mandatory on line electronic registration service
- Other bodies who use PSN or other secure networks could refuse to share

information with us (because to do so would put at risk their PSN compliance)

Please note the Cabinet Office have re-emphasised that no longer will we be allowed to fail and given time to submit and enact a remedial action plan in a letter issued in June 2013 it said “The mandate exists to suspend organisations that fail to reach compliance”. On 4 October they further reviewed this and agreed to allow councils more time to achieve compliance in 2013 only; but that the Zero Tolerance would remain for future code of compliance submissions.

3.2 In addition to the PSN compliance the 2012 audit of the Council undertaken by the Information Commissioner, and the follow up review to that audit; and the 2013 audit undertaken of our use of the CJSM system by the Ministry of Justice auditors both introduced new and extended or clarified existing information security obligations. Having had such audits and been given time to rectify weaknesses we are at increased risk of both non-compliance or of tougher penalties should a future security breach occur.

3.3 The proposed increased checks before staff are employed in effect extend existing checks beyond a small group of employees to all employees over the next 3 years. These checks are less extensive than Criminal Record Bureau checks.

3.4 There has been considerable response to these new tougher controls which has led to some clarifications and some relaxations. Peer networks including the Society of IT Managers (SOCITM) are working with the Cabinet Office to try to achieve further practical changes and lobbying by a range of peer networks does help. To continue to use local government networks to provide feedback to the compliance authorities seeking:

- a more consistent audit regime
- a more practical application of the requirements, reducing the costs of compliance
- For future changes to be better planned and for the additional funding to be made available to support compliance

SUPPORTING INFORMATION

4.1 See Appendix 2

OTHER OPTIONS CONSIDERED

5.1 Don’t apply these stricter rules and take the risk of having access suspended. This is not an option in the near future, but should the Council decide to share such services we could either adopt such an approach and pass on the responsibility to the shared service provider; or we could seek to offer such services to other Councils who are struggling to achieve and maintain their own PSN and CJSM Zero Tolerance compliance certification.

5.2 Implement further segregation of both ICT networks and of building management arrangements such that all staff to whom such compliance regimes apply are not co-located or share common offices, data networks or mailing systems. This is contrary to one Derby one council, to new ways of working and would not work in practice. It would become more impractical as compliance is extended to more aspects of the Council's work.

This report has been approved by the following officers:

Legal officer	Janie Berry – Director of Legal and Democratic Services
Financial officer	Toni Nash – Head of Finance (AHH and RES)
Human Resources officer	Hannah Parry – HR Operations Manager
Estates/Property officer	
Service Director(s)	
Other(s)	Glyn Peach – Head of ICT Miles Peters – Infrastructure Manager Alison Moss – Information Governance Manager

For more information contact:	Nick O'Reilly 01332 64-3254 nick.oreilly@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 – Detailed Requirements Appendix 3 – Baseline Personnel Security Standards Appendix 4 – Visitor Management

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 The additional costs of compliance are :

Description	Initial	On-going
Access logging tools, email protective marking and addition technical security	£ 125,000	£ 25,000
Pre compliance health check	£ 0	£ 15,000
On Line Policy and Training System	£ 0	£ 75,000
Total	**£ 125,000**	**£ 115,000**

The initial costs will be funded form the budget risk reserve and the on-going costs from the corporate contingency budget.

1.2 Failing any of these compliance audits will have a much larger financial impact on the Council as the costs of delivering the required services by non electronic means would be much larger; and the damage to the Council's reputation if we fail an audit would be equally significant. All of the above measures also act as a significant factor to mitigate any enforcement action or penalty notice following a security breach. The latest security breach involving data being published is an example; if the employee had completed the on line policy and we had an audit record of such it would mitigate any finding.

Legal

2.1 Failure to apply these extended security arrangements may increase the risk of not complying with one or more legislation, most notably the Data Protection Act.

2.2 The HMG Baseline Personnel Security Standard describes the pre-employment controls that must be applied to any individual who has access to government assets. Its rigorous and consistent application also underpins national security vetting.

Personnel

3.1 The additional compliance requirements will have implications for staff; in particular:

a. For all staff with computer access to complete the on line policy training and verification.

b. For all new staff and all existing staff with PSN access to undertake baseline Personnel Security Checks.

c. For managers to ensure that the policies are being followed and that staff are aware of requirements in respect of managing data, data classifications and protective marking and use of government datasets.

3.2 Applying the BPSS will ensure pre-employment checks controls are tighter and will provide assurance and confidence that risks are being appropriately managed.

Equalities Impact

4.1 None - BPSS will be applied equally to all staff where such is required from 2014.

Health and Safety

5.1 None

Environmental Sustainability

6.1 None.

Property and Asset Management

7.1 None.

Risk Management

8.1 The new controls are all aimed at reducing risks; risks of technical network security breaches; risks of organisation security breaches and risks of failure to comply with regulations or data protection obligations. The Cabinet office Zero Tolerance letters make it clear that central government view these as being fundamental changes required to reduce risks.

Corporate objectives and priorities for change

9.1 Maintaining compliance certification helps protect a number of high profile and critical services and to maintain the reputation of the Council. Failing to achieve this could be as damaging as failing other inspection and audit regimes.

Appendix 2

Detailed Requirements

Introduction

1.1 The Zero Tolerance approach imposed by the Cabinet Office changes the landscape in that any future failure to comply may result in immediate suspension of access to central government systems including those used to process benefits, for electoral registration and for youth offending. Previously failure resulted in us being given a specified time limit within which we had to take corrective action and achieve compliance.

1.2 The impact is that for a number of compliance criteria where stricter rules have been mandated, we need to introduce new controls and safeguards which incur additional costs.

1.3 The zero tolerance approach was launched by the Cabinet Office on 29 April 2013; however at that time it was unclear exactly what was meant by zero tolerance, what additional security controls would be required and how much these would add to the costs. Since 29 April there have been a number of clarifications and considerable attempts by the local government Chief Information Officer Council to reduce the impact:

27 June	Compliance update and initial response – some FAQ’s
31 July	Supporting transition new help launched
6 August	End user device security action notice and revised compliance guidance notes
12 August	Unmanaged endpoint gap analysis guidance note
19 August	Compliance statement template and self-assessment issued with further guidance
23 September	Baseline Personnel Security standard requirements issued – new requirements stated for 2014 and 2015
29 September	Bring Your Own Device and Secure Remote Access Guidance
4 October	Revised compliance regime issued
16 October	Unmanaged endpoint gap analysis assessment toolkit with 14 defined rules
6 November	Security Architecture event to assist with complaint network design
11 November	Electoral Registration network accreditation clarified

In other words although zero compliance was flagged back in April; its implications and additional requirements identifying extra costs have emerged over the months that followed. To some extent this is due to the compliance audits being undertaken and the feedback they have provided. It is the case that better support and guidance has been issued and some aspects have been clarified which reduces the potential cost. Both the guidance now available and the information shared between local authorities means only now can we prepare sensible and fully costed proposals for what this means for Derby City.

1.4 Compared to many other councils we are in a strong position, we passed our compliance audit for 2013/14 (the third to do so) and have good security in place. However there are new requirements for us in 2014 and we would not pass the compliance without meeting these. The impact would be serious meaning we could no longer access government data needed to process benefits or for on line electoral registration.

1.5 In addition to the PSN compliance the 2012 audit of the Council undertaken by the Information Commissioner, and the follow up review to that audit; and the 2013 audit undertaken of our use of the CJSM system by the Ministry of Justice auditors both introduced new and extended or clarified existing information security obligations. Having had such audits and been given time to rectify weaknesses we are at increased risk of both non-compliance or of tougher penalties should a future security breach occur.

IMPACT AND MITIGATION ACTION REQUIRED

2.1 Failing to achieve these could mean we can no longer access systems needed to:

- Our access to the PSN network will be suspended
- We can no longer access government data required to process benefits and/or to investigate suspected fraud
- We can no longer access the mandatory on line electronic registration service
- Other bodies who use PSN or other secure networks could refuse to share information with us (because to do so would put at risk their PSN compliance)

2.2 Failing to apply these controls could also lead to higher risks should any security breach occur, with an increased risk of financial penalties form the Information Commissioner's Office.

2.3 Failure of a compliance submission would lead to temporary suspension of access and being unable to meet some statutory duties; it could also lead to significant damage to reputation. Thus we need a more rigorous approach pre compliance submission.

2.4 Whilst we will endeavour to comply with such Zero Tolerance compliance requirements, where such cannot be easily met initially and where a partial compliance is allowed then both a risk assessment and a proposed mitigation plan will be produced for consideration by the Information Governance Board (or by Chief Officer Group).

2.5 To implement the following increased technical security measures in order to comply with the current Zero Tolerance requirements:

a. An active logging tool, replacing passive monitoring.

b. Baseline Personnel Security Checks for all new employees and all new agency/contract staff.

c. An email protective marking tool that will force users to add a protective marking classification to all outgoing external emails.

d. Stricter secure remote access controls for staff, partners suppliers and members including some use of two factor authentication.

e. Enforce stricter endpoint device controls (computers, smartphones etc) on all devices accessing council business networks or that can receive council email such that only council provided devices or devices that the Council has been able to enforce required endpoint security controls can access the data network.

f. Enforce stricter rules that prevent users who access the PSN, the CJSM or the Egress secure mail facilities from forwarding such emails to non-secure council mailboxes.

2.6 To re-enforce the need for improved organisational security measures including policies, procedures and training that include:

a. All staff with access to electronic data to complete and accept relevant policies and training on the new e-learning portal and for this to be a requirement for all new staff; failure to pass the Information Security Policies may lead to suspension of some or all access.

b. The implementation of document classification and protective marking both through the corporate EDRMS and on other documents.

c. The reporting of all potential security incidents such that these can be assessed and managed in accordance with all relevant compliance regimes.

d. The completion and annual review of information asset audits and the application of both protective marking and record retention schemes to relevant information assets.

e. To undertake an independent pre compliance review once a year that covers the PSN, CJSM and PCI compliance requirements.

f. To ensure that all third parties including suppliers, partners and trade unions given access to our network sign and adhere to a Memorandum of Understanding that specifies the terms of access.

g. To enforce stricter visitor management controls at all Council premises that ensure no visitor can access staff areas without verification of their identity.

h. To introduce a revised remote access policy that requires staff accessing the PSN or CJSM networks not to do some from public wireless services unless they have been set up with 2 factor remote access security.

2.7 To allocate funding from within the Resources Budget for the additional compliance measures in a separate information security budget that will be ring fenced from any future savings targets with :

Description	Initial	On-going

Access logging tools, email protective marking and addition technical security	£ 125,000	£ 25,000
Pre compliance health check	£ 0	£ 15,000
On Line Policy and Training System	£ 0	£ 75,000
Total	**£ 125,000**	**£ 115,000**

2.8 To agree that where increased charges are per user or per employee these will be funded by the respective services. These include:

- Baseline Personnel Security Checks
- Remote access two factor authentication
- Secure partner email access
-

These are all priced per user with details included in section 4; information on costs will be maintained by the Information System department for technical issues and by the Human Resources department for personnel issues.

LOBBYING FOR CHANGE

3.1 In effect as a council that has duties including benefits and electoral registration we have little choice to comply in the short term. However there may be particular security controls that we could seek to mitigate or to apply to some but not all staff (or to some but not all buildings). The Zero Tolerance regime extends security to all users on the PSN network and to physical security and visitor management in all premises where either PSN related data or criminal justice information is processed.

Often these tighter security compliance rules are not popular, and we can come under pressure to relax such or to exempt certain users from them. With a Zero Tolerance approach such exemptions may not be possible in future; or will need explicit approval by senior management. This may include having to remove some exemptions currently applied to Members, Chief Officers and Trade Unions. The Zero Tolerance approach includes not sharing log on access or passwords.

3.2 There has been considerable challenge to the way these Zero Tolerance compliance rules have been implemented, and local government networks including the Society of IT Managers - SOCITM, The Local Government CIO Council and Benefits Officers have made a series of representations to the Cabinet Office. Some changes to the timescale and approach to applying this have been offered in response but not to the underlying Zero Tolerance approach. However it is important that where such an approach creates extra cost or other barriers for councils we continue to use our networks to seek further modifications; and these may need to include more representation through Chief Executive, Chief Officer and elected Member networks.

3.3 The compliance authorities do offer guidance, and have taken on board some feedback; however we need to maintain this challenge especially as the compliance rules also change each year. We will need to reconsider tools such as encryption, web and email filtering, virus and malware detection and intrusion prevention tools as both technology and risks change.

SUPPORTING INFORMATION

4.1 The PSN Zero Tolerance compliance rules and the Cabinet Office Security Framework are available on their respective websites. There are too many documents to reproduce or to attach as appendices.

https://www.gov.uk/public-services-network
https://www.gov.uk/government/publications/security-policy-framework

The CJSM rules require registration to access detailed rules but is high level information is also available on the website http://cjsm.justice.gov.uk/

There is also advice and guidance on the Information Commissioners Office website http://www.ico.org.uk/

The Payment Card Industry Standards although not specifically covered by this report are also available at https://www.pcisecuritystandards.org/

4.2 The ICO audit and resulting action plan and the CJSM Audit and resulting action plan are held by the Information Governance Manager and copied to relevant officers who are involved with the relevant compliance process or completing actions. The technical security and compliance submissions for the PSN, CJSM and PCI regulations are prepared, stored and submitted by the Infrastructure Manager in the ICT department.

4.3 The active logging tool proposed will assist with us achieving compliance with each of the PSN, CJSM and PCI requirements. There is a cost of £40,000 and an annual cost of £10,000 a year and this is a new growth pressure. We had been using an alternative of passive monitoring which is now deemed to high risk. The CJSM audit requirement is "Derby City Council must enable the logging of who has accessed the CJSM service such that they are able to trace any security breaches" and there are equivalent PSN and PCI requirements. In both of the last two years we had failed either the PSN or PCY submission due to passive rather than active logging.

4.4 The requirements in the PSN to extend Baseline Personnel Security checks have been reviewed by the Human Resources department and a separate report is attached as Appendix 2. This will incur additional pre-employment checks for all new employees and agency staff. The check is of identity, nationality and immigration status, employment history (three years) and verification of Criminal record (unspent convictions only). This needs to be applied to all staff that accesses our data network; it used to only apply to staff in the benefits service or with access to the PSN email service. The requirement to comply commences from 2014 for staff accessing secure email (PSN, CJSM) and from 2015 for all staff with network access. The cost of this is £25 per check and to manage this process it is recommended this should be implemented for all new starters from 2014.

4.5 Currently the only way we can add a security classification or protective marking on outgoing emails is for users to add such manually. Some users have been set up to share secure information via email with partners using a tool called Egress switch.

However this does not prevent emails being sent to other parties without a classification. Estimates for an email protective marking tool that forces users to select a protective marking category before sending email are £40,000 to implement and £10,000 a year.

4.6 The stricter access controls for staff and members means we have to remove facilities such as Outlook web Access from the insecure remote portal (we have already committed to do this in response to the ICO audit report) and only offer this through either the Citrix Remote Access Gateway or by other similarly secure means. This means that users not yet migrated to the Citrix environment will be unable to access their council mailbox remotely. Currently this is roughly half of the user population, but as we extend the new ICT environment to Stores Road and to Roman House the number without access to email remotely will reduce.

The stricter access for partners and suppliers is more complicated. For any supplier we provide remote access to our network in order to undertake support of systems we will need to ask them if they are PSN compliant certified; and we will need a memorandum of understanding that agrees controls on how they access our network. For suppliers without a PSN certificate we need to lock down access to specific network locations (which is what we already do).

For partners there is an even bigger challenge in that the application of end-point controls means that no partner can access our council business data network unless they either have a PSN certificate themselves or we can control their endpoint device; in effect their computer. This would affect partners who share our buildings (Including Derby Homes, the Museums Trust, Action for Children, Derby Health-watch) or who use customer access points in our reception. Most partners will be unwilling to do this for very good reasons. Partners can use the public wifi network in the Council House and provided they can do what they need with their own remote access gateway tools can continue to use our buildings. Schools are not affected as the Schools network is already separate.

4.7 The stricter rules also mean we need to return to a policy of requiring two factor remote access in three cases:

a. For all staff who access government data across the PSN (currently benefits, electoral registration and some IS staff)

b. For all staff that use either the PSN or the CJSM secure email services; including staff involved with youth offending.

c. For all staff including council provided laptop users who use Virtual Private Networks rather than the Citrix Remote Access Gateway.

The costs of this are £40 a year with a minimum 2 year contract; any such request would need to be funded by the service.

4.8 Endpoint controls under the new Zero Tolerance regime mean that:

- Users (including members) can only use non council smartphones to receive email if they agree we can reset their phone and ensure the phone can be remotely wiped if it is reported lost or stolen and if the employee leaves the Council. This is our current policy

- Users can only use non council devices on our business data network if they do so via our secure Remote Citrix gateway; or if they agree that the Council can wipe their computer device back to factory settings and install our security tools.

- External users can continue to access the public (Guest) network in the Council House and use the internet to access their own business data, but cannot do this from our non-Guest network.

- We can enforce rules that prevent the copying of council data or emails from the network to a local drive on the computer or to any portable media.

In essence this means where we want to promote Bring/Use Your Own Device (B/UYOD)we can do so, bit we need to invest in tools that provide higher levels of security. Some of these involve enhancing our gateway security and others individual device security. There is a commitment from the Cabinet Office to develop new guidance on B/UYOD during 2014 such that the Zero Tolerance rules do not become a barrier to such.

4.9 Because of the new Endpoint controls where we intend to allow other tenants to share, or to provide some services from within council buildings this can only be done if:

a. We provide a separate data network for them to use

b. They can use the a guest network set up for such purposes

c. If they agree to us providing and managing any computers they use when within our buildings.

This does impact existing tenants including Derby Homes, The Museums Trust and Derby Health-watch. It is proposed to ask each to sign a Memorandum of Agreement agreeing that they will only use devices that have been provided via the Councils ICT service, and which will be managed and controlled by IT staff authorised by the Council.   In effect this extends the current working agreements we have with each, making it more formalised; if any of them wanted to manage their own computers or supply their own devices they would have to leave our data network.

This also extends to other parties including the trade unions, some of whom currently supply some of their own computer devices, and to partners using the customer reception area. We have two choices for such:

a. we allow them to use thin client terminals or laptops and network printers supplied and managed by the Council

b. they have to use the guest network and not the business network.

4.10 We can implement blocks on users to prevent them forwarding mail from a secure mailbox to a council mailbox; but we cannot prevent them from forwarding such to their own non council mailbox (although to do so would be a breach of our policies).

In order to do this for all users who have a secure email facility we will need to provide them two different mailboxes, whereas currently for some the emails are within one mailbox. This will be provided to such users by means of separate mail shortcuts. There is no extra cost, but it does mean users having to use and monitor two mailboxes.

4.11 The new on line portal for reviewing policies and for undertaking both policy and other training has met the requirements of three separate compliance audits (PCI, ICO and External Audit). This is an important tool; however the audits require that such policies are re-confirmed annually, this does not mean repeating the full process but users verifying they have checked for any changes and read any new policies. Without this we had no audit record of users agreeing to such policies. The Information Security Policies are mandatory and we will need to consider what action to take where users do not review these and pass the end of review tests. Any PSN user who fails will need to have their PSN access suspended.

4.12 We have committed to applying document classification more rigorously in our response to the ICT audit. We have a tool in the new EDRMS that allows the application of such and that can also help with marking record archiving and retention triggers. However there are still many documents and records outside of this tool. One step we could make is to circulate some word and excel templates that include a header or footer that adds a document classification/protective marking field (but users would still have to fill this in). Similarly we should require all reports generated from application software to have the option to add a classification/protective marking statement and require that suppliers include such a facility in any future release. Where we develop and write our own reports and documents from systems we should include a similar protective marking scheme.

4.13 We need to reinforce the process for reporting all security incidents, and that we have a robust process for assessing these and deciding if they need reporting to the Information Commissioner, to another compliance body or can be managed internally. When the existing process is used it does work, but there is a fear that often incidents go unreported. Staff may need to be re-assured that unless there is a deliberate security breach or a case of gross negligence it is better to report such incidents such that mitigation action can be taken.

4.14 The appointment of Information Asset Owners and the process of an initial information asset audit is underway; and we are making progress with both protective marking and record retention/archiving/deletion schemes. The Zero Tolerance approach re-enforces the need for these and as such they need to remain a priority. These should be reported back to the Information Management Group.

4.15 Because the Zero Tolerance regime moves from one that allows for rectification and resubmission before any suspension of access to one that may result in full or partial suspension upon failure it means we need to reintroduce pre submission independent tests, we used to do this but it was stopped due to financial pressures. An estimate of £15,000 a year.

4.16 We need to review and replace existing 3rd party access agreements with new agreements that meet the zero compliance requirements. This will add additional security burdens to all such 3rd parties. This will require different agreements depending on what access we give each supplier; however there will be some common requirements. A new template will be prepared. Suppliers who access systems that process government data (benefits, electoral registration) should be required to show their PSN or equivalent security certificate; the PSN does require suppliers to achieve this. This may be more onerous for suppliers and third parties who do not access such data because the Zero Tolerance approach means we have to extend some new controls to them.

4.17 Each of the PSN, PCI and CJSM compliance requirements includes statements on physical security. This has included that visitors must not be able to access staff only areas without being first met at reception and given a visitor badge. The latest CJSM audit has extended this to add a further requirement to check the identity of a visitor first. This applies to all sites where CJSM mail can be accessed, and as such includes the Council House. If a visitor arrives that a member of staff knows and was expecting all they need to do is meet them and ensure they have a valid visitor badge. If a visitor arrives that is unknown then we should ask for some form of identification that allows us to check they are who they say they are, in effect some form of photo id. This means we cannot use automated visitor management machines without additional identity checks. It also means that all visitors must still remain on the customer side of any entrance until they are met by a member of staff. A separate briefing note has been provided and is attached as Appendix 3.

4.18 The PSN code of compliance includes an explicit requirement for staff not to use public wifi networks where they can enter their user name and password unmasked. The guidance gives an example of using wireless networks in coffee shops, but this equally applies to other public wireless networks including those on trains. This can be permitted if the user name or password is masked (which is not something we can control) or if in addition to a user name or password there is a requirement for a 2 factor authentication device. We need a new policy or to amend an existing policy to comply.

Appendix 3

Baseline Personnel Security Standard (BPSS)

SUMMARY

1.1 Issued by the Cabinet Office, BPSS is the minimum standard to ensure the identity and integrity of an employee who has access to official information via a Public Services Network (PSN). It involves four main elements:

- Identity check
- Nationality and immigration check
- Employment history (past 3 years)
- Verification of Criminal Record (unspent convictions only)

1.2 Compliance is expected in 3 stages:

- 2013 – all users of PSN service or data
- 2014 – all users of PSN email
- 2015 – all users of a PSN connected network

Derby City Council has already complied with the 2013 stage. Due to the way the Derby City Council email service works, the Council will need to meet the 2014 level of compliance.

1.3 As BPSS describes pre-employment controls the responsibility for applying BPSS will tend to rest with HR.

A range of pre-employment checks are currently undertaken by Derby City Council but BPSS requires a tighter control across a wider range of employees.

1.4 It should be noted that the criminal records verification element of BPSS raises a financial concern. Currently Disclosures can only be carried out for posts that legally meet the requirements to do so and these look at spent and unspent convictions.

The cost of all Disclosures is met by the employing department.

The BPSS requirement will require a Basic Disclosure on all other council posts not already subject to a Disclosure; this will only look at unspent convictions. This currently is only done through Disclosure Scotland at a cost of £25 per person.

To illustrate the impact, since April 2013 there have been 347 new employees join Derby City Council who would be subject to BPSS compliance. Of these only 67 have required a Disclosure, therefore 280 Basic Disclosures at a cost of £7,000 would have had to be carried out to ensure compliance with BPSS.

RECOMMENDATION

2.1 To conduct a full audit of current recruitment practices and identifies areas for immediate improvement to ensure compliance for 2014, especially regarding the recording of pre-employment checks.

2.2 To ensure compliance, BPSS checks will need to apply to all recruitment activity including internal transfers and use of agency/contract workers. Contracts with contractors/agencies will need to be reviewed in line with BPSS requirements to ensure checks have been carried out satisfactorily and that these may be audited

2.3 To develop a recruitment policy and associated processes that clearly explains the Councils commitment to meeting BPSS and the steps that will be taken before allowing an individual to commence employment.

REASONS FOR RECOMMENDATION

3.1 Derby City Council will need to ensure evidence is available to show compliance with BPSS. It is fully expected that the new HRIS will be used to record all pre-employment checks and force full compliance through tighter process controls.

3.2 There is no expectation to carry out checks retrospectively but they will need to be done where assurances have not been obtained or are in place to allow for access to government assets.

SUPPORTING INFORMATION

4.1 HR Operations administers the recruitment process for Derby City Council however there is great reliance on the appointing manager to collect a variety of evidence from the candidate at interview. This is not always obtained or thoroughly and HR often has to chase candidates for the correct information in order to carry out the required checks. This then delays the process.

A snapshot looking at current processes indicated that:

- There does not seem to be concerns regarding Identity checks.
- Immigration and asylum checks are done to check to see if the paperwork is present but it is felt to be the appointing manager's role to verify right to work. Where the candidate is a Non EEA national HR do carry out extra checks, but they do not currently cover all the UK Border Agency regulations.
- Employment History this is collected as part of application process but gaps are not identified or filled by HR. Appointing managers are expected to explore gaps at interview.
- And again questions regarding convictions are part of application process but nothing done with this data by HR. Appointing managers are expected to explore concerns if highlighted as part of a Disclosure discussion

The review will clearly need to look at the responsibility of the appointing manager in their recruitment, the overall process and how best to carry out pre-employment checks to ensure compliance with BPSS.

OTHER OPTIONS CONSIDERED

5.1 None – the personnel security controls **must** be applied to any individual who, in the course of their work, has access to government assets.

This report has been approved by the following officers:

Legal officer	
Financial officer	
Human Resources officer	Hannah Parry, HR Operations Manager
Estates/Property officer	
Service Director(s)	Karen Jewell, Director of HR & Business Support Nick O'Reilly, Director of ICT
Other(s)	

For more information contact:	Hannah Parry, HR Operations Manager 01332 643511 hannah.parry@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications

Appendix 4

1 Background

1.1 This briefing note explains the security considerations and the constraints we have to impose in managing visitors to Council buildings. This has been written both because of the proposed new visitor management system in the Council House and due to the higher levels of security (“a zero tolerance approach”) being adopted by the Cabinet Office and by the Ministry of Justice.

2 General Security

2.1 It is accepted that we have a duty of care to our staff to ensure visitors to all Council premises are managed effectively. This includes reception arrangements, issuing visitor badges and policies that no visitors should be unaccompanied. The exact arrangements vary depending on both the building and the functions being carried out.

2.2 It is also accepted that we need security on access to information be these paper files or data held electronically. Policies and procedures such as clear desk; locking files or offices overnight; a lockout timer on computer screens and positioning computers to avoid them being read by visitors all contribute to this.

3 Higher Levels of Security

3.1 Higher levels of security are required to meet a number of obligations either imposed through a compliance regime or following audit inspections. These include:

i) The Cabinet Office HM Government Security Framework
ii) The Cabinet Office Public Sector Network Code (PSN)) of Compliance
iii) The Ministry of Justice Code of Compliance and Audit Recommendations
iv) The Payment Card Industry (PCI) standards
v) The Information Commissioners Office advice, guidance and Audit Recommendations

3.2 In the last 12 months each of the Cabinet Office, the Ministry of Justice and the Information Commissioners Office have issued revised rules or audit recommendations requiring higher levels of security. These do not just apply to data security or to security of the ICT networks, but also to physical building security.

3.3 Each one of these requires some level of minimal controls on the management of visitors. In issuing revised rules and in adopting “a zero tolerance approach” one of the new or clarified requirements is to apply such controls not just staff and building zones where confidential data is processed but to the entire perimeter. Examples of the controls are given in the Appendix.

i) For ICT this means extending controls to all staff not just staff that process benefits, handle debit or credit card payments, manage social care information or process employee data.

ii) For building security and visitor management that means applying controls on all public access points into a building. It does not apply to exits that cannot be opened from outside or to fire and evacuation doors.

3.4 In most cases the compliance auditor's clarification or interpretation of the requirement extends the security level such as a need to check the identity of a visitor before they gain access to a staff only area and that visitors are met at the reception and escorted to and from their meeting. Visitors should where practical be issued with a visitor badge.

3.5 The highest requirement imposed by the latest Ministry of Justice Audit inspection goes furthest. It requires all visitors to any building where staff access and use the Criminal Justice Secure Email (CJSM) system to be verified by checking their identity (the implication is this means some form of photographic id). Council Officers involved with this audit agreed to this recommendation because if they had not we would have been unable to access the CJSM system which is critical for managing matters going to the courts, in particular in respect of youth offending. Most of these staff work at Middleton House/29 St Mary's Gate with their own separate reception but some staff in the Council House can and do access the CJSM system and therefore the same controls apply.

4 Visitor Management System

4.1 The higher level security does not mean we cannot or should not introduce the new visitor management system, but does mean we have to impose some constraints upon it.

4.2 Any automated kiosks that issue badges to visitors must be located on the customer/public side of any entrance, and not within a secure staff area. The visitor verification taking place before access to a secure area.

4.3 Until a visitor is met by a member of staff then visitors should remain on the customer/public side of any entrance or in a managed reception facility inside the staff area where they cannot access staff areas where personal data of any kind is processed and where access to any government data set is potentially available.

4.4 On sites where CJSM mail is processed (and very possibly in future where data such as benefits or health records) are processed visitors should be asked to show some form of photographic identification. This needs to be explained to visitors before they arrive. This includes the Council House.

4.5 There is not currently a need to take photographs or to issue photo identity badges for visitors.

4.6 All Visitor Badges should have a date or dates valid printed upon them, and the visitor management system needs to be able to do this.

4.7 It is important that all visitors' badges are retrieved such that they cannot be reused by another person once their valid date has expired.

5 Implications of Not Following these Requirements

5.1 We risk the possibility of failing a code of compliance submission and therefore having our access to critical systems required to fulfil various business functions suspended or withdrawn. The functions include:

i) Court Proceedings where data has to be transmitted using the CJSM system (mainly youth offending)

ii) Processing Benefits where access to government data via the PSN is mandatory.

iii) Processing credit and debit card transactions.

Note all of the above involve annual submission of a code of compliance and an annual audit to check we are complying.

5.2 The risk that should an incident occur we could be reported to the Information Commissioners Office which continues to increase the levels of penalties in the form of fines levied for breach of data security.

5.3 The risk that partners with whom we have data sharing agreements may require further evidence of better physical building controls in order to continue sharing data with us.

5.4 All of these are risks that can be considered against the inconvenience to visitors and the additional costs of imposing higher levels of visitor management security. However if we choose to accept such risks in respect of access to central government data or systems (CJSM, PSN) or payment card transactions then we would need to report such in our compliance submission and in response to any future audit. This may lead to further instructions from the compliance authorities.

Appendix – Compliance Statements on Building Security or Visitor Management

The following table gives extracts from various security compliance requirements. It is notable that many of these are none specific; it is not necessarily the compliance requirements but the way these are being interpreted and applied by different compliance auditors. The audit regime is leading to higher levels of security being mandated than the compliance document suggest.

Compliance Body/Mandate	**Requirement**
Cabinet Office – HMG Security Framework	*Access Control:* Put in place arrangements to control and monitor access to their estate. Frontline staff (security guards, receptionists etc) have a key role but must be supported by appropriate technical and procedural controls, potentially including: ▪ Automatic Access Control System (AACS); ▪ Pass or ID system; ▪ Visitor control and escorting policy; ▪ Pass activated doors, turnstiles etc; ▪ Entry and exit searching; ▪ CCTV; ▪ Vehicle Barriers and Vehicle Identification Passes. Buildings containing protectively marked or other valuable assets should have as few entry and exit points as business functions and safety will allow. Have effective plans or procedures in place for dealing with and intercepting unauthorised visitors, intruders or suspicious items. Such plans must include the ability to systematically search and cordon off areas of the establishment if necessary.
Cabinet Office – PSN Network Zero Tolerance April 2013	**We're raising the bar on Compliance enforcement** Before your organisation can be connected to PSN or use it to receive PSN Services, you must be accredited and achieve PSN Compliance; **no Remedial Action Plans or weak compliance positions will be imported into PSN.** We are ceasing the issue of Remedial Action Plans and any oversight of actions arising from an On-Site Assessment or IT Health Check – **you will either be assessed as compliant or rejected**. All Local Public Services should ensure the security of their information through the physical security of their buildings, premises and systems. There should be regular assessments of physical risks to information, which are then discussed by senior management. Physical security should be layered so

PSN – Local Data Handling Guidelines	that the most important processes are undertaken in the most secure areas. The connecting organisation shall ensure that physical access to buildings and rooms holding PSN equipment and terminals are secured in line with the recommendations in the guidance notes provided: Recording all visitors to buildings and, wherever feasible, ensure that they are accompanied whilst on the premises. Implementing a clear desk/clear screen policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are unattended.
Ministry of Justice – CJSM Audit at Derby 2013	Derby City YOT should introduce a procedure whereby all visitors have their ID checked before being issued with visitor passes.
Information Commissioner's Office Audit at Derby 2012	**c23.** Physical security into the current buildings was of a high standard. Buildings had internal swipe cards controls allowing access into zoned areas. **c24.** Currently visitors are required to sign in whenever they arrive at a Council office and are accompanied at all times. However, they are not issued with identity badges to identify them as visitors. **Recommendation:** Ensure that a visitor policy is in place and that it is adhered to. **Management Response:** Agreed - We will introduce a visitor policy for the whole Council and consider introducing visitor badges at all Council buildings. **Implementation Date:** end December 2012
Information Commissioner's Office – The Guide to Data Protection	**24** Physical security includes things like the quality of doors and locks, and whether premises are protected by alarms, security lighting or CCTV. However, it also includes how you control access to premises, supervise visitors, dispose of paper waste, and keep portable equipment secure.