Public Document Pack

Gedling Borough Council

Civic Centre,
Arnot Hill Park,
Arnold,
Nottinghamshire,
NG5 6LU

Agenda

Cabinet

Date:	**Thursday 17 December 2015**
Time:	**12.30 pm**
Place:	**Reception Room**

For any further information please contact:

Lyndsey Parnell

Senior Elections and Members' Services Officer

0115 901 3910

Having trouble reading this? Please call 0115 901 3910 if you need it in large print, audio or another format.

Cabinet

Membership

Chair	Councillor John Clarke
Vice-Chair	Councillor Michael Payne
	Councillor Peter Barnes Councillor David Ellis Councillor Kathryn Fox Councillor Jenny Hollingsworth Councillor Henry Wheeler
Observers:	Councillor Chris Barnfather

AGENDA

Page

1 **Apologies for Absence.**

2 **To approve, as a correct record, the minutes of the meeting held on 12 November 2015.** 5 - 10

3 **Declaration of Interests.**

4 **Retaliatory Eviction and the Deregulation Act 2015** 11 - 14

Report of the Food, Health, and Housing Manager.

5 **The Smoke and Carbon Monoxide Alarm (England) Regulations 2015 - statement of principles for determining financial penalties** 15 - 24

Report of the Food, Health, and Housing Manager.

6 **Update to the Information Security Policy** 25 - 94

Report of the Research and Development Manager, ICT Support and the Council Solicitor & Monitoring Officer.

7 **Progress Reports from Portfolio Holders.**

8 **Member's Questions to Portfolio Holders.**

9 **Any other items the Chair considers urgent.**

This page is intentionally left blank

MINUTES
CABINET

Thursday 12 November 2015

Councillor John Clarke (Chair)

Councillor Michael Payne	Councillor Kathryn Fox
Councillor Peter Barnes	Councillor Jenny Hollingsworth
Councillor David Ellis	Councillor Henry Wheeler

Observers:	Councillor Chris Barnfather
Officers in Attendance:	J Robinson, H Barrington, S Bray, M Kimberley, D Wakelin and A Dubberley

42 APOLOGIES FOR ABSENCE.

None.

43 TO APPROVE, AS A CORRECT RECORD, THE MINUTES OF THE MEETING HELD ON 22 OCTOBER 2015.

RESOLVED:

That the minutes of the above meeting, having been circulated, be approved as a correct record.

44 DECLARATION OF INTERESTS.

None

45 EAST MIDLANDS DEVOLUTION DEAL

The Chief Executive introduced a report, which had been circulated prior to the meeting, updating Cabinet on progress made towards a devolution deal for the East Midlands.

He explained that just prior to the meeting he had received word from central government that due to concern from backbench MPs, a deal for this area was currently 'paused' and further information would be available at an area meeting scheduled for Friday. He added that the recommendations the report remained relevant as negotiations on the deal would continue and Councillors would be kept informed throughout the process.

RESOLVED to:

1) Note the progress towards a devolution deal for Derbyshire and Nottinghamshire;

2) Recommend to Council that delegated authority be given to the Chief Executive in consultation with the Leader of the Council and Leader of the Opposition to continue negotiations and to sign the devolution deal, subject to ratification of the deal by the Full Council;

3) Ask the Chief Executive to continue to provide regular updates to all Councillors on the progress of the deal; and

4) Note that a report to consider the final agreement of the deal will be brought to Full Council after the necessary changes in legislation and conclusion of a detailed deal document.

46 GROWTH AND INFRASTRUCTURE BOARD

The Chief Executive introduced a report, which had been circulated prior to the meeting, that proposed the establishment of a Growth and Infrastructure Board to oversee the development and progress of key initiatives and areas of work that underpin the economic and housing growth of the Borough.

RESOLVED to:

1) Approve the arrangements for establishing a Growth and Infrastructure Board as set out in section 2.1 of the report; and

2) Review the effectiveness of the Board in 12 months.

47 REFRESH ORGANISATIONAL DEVELOPMENT PROGRAMME

The Chief Executive introduced a report, which had been circulated prior to the meeting, updating Cabinet on the work of the Refresh Board.

RESOLVED to:

1) Note the progress on the Refresh organisational development programme detailed at Appendix 1 to the report;

2) Endorse the vision, values and priorities set out at Appendix 2 to the report, noting that these would form part of the Gedling Plan to be approved at a later date by Cabinet and Full Council; and

3) Endorse the Gedling Employee, Manager and Leader Standards set out at Appendix 3 to the report.

48 QUARTERLY BUDGET MONITORING, PERFORMANCE DIGEST & VIREMENT REPORT

Mark Kimberley, Corporate Director, introduced a report, which had been circulated prior to the meeting, informing Cabinet of the position against Improvement Actions and Performance Indicators in the 2015/2016 Gedling Plan, updating Cabinet on the likely outturn of the Revenue and Capital Budgets for the 2015/2016 financial year and seeking approval for changes to targets and budgets as outlined in the report.

Specifically on the request to amend targets for recycling in the Borough Members stated that they were not minded to approve the request to reduce the targets as they felt that reducing such targets in year would send the wrong message on such an issue.

RESOLVED to:

1) Approve the General Fund Revenue Budget virements included within Appendix 1 to the report;

2) Approve the changes to the Capital Programme included in paragraph 2.2.3 of the report;

3) Note the virements and transfers to/from reserves and funds during the last quarter as detailed in appendices 3 and 4 to the report; and

4) Include details of budget and performance monitoring in a quarterly performance digest, to be published on the Council's website and Intranet in line with the recommendations of Performance Review Scrutiny Committee.

49 PRUDENTIAL CODE INDICATOR MONITORING 2015/16 AND QUARTERLY TREASURY ACTIVITY REPORT FOR QUARTER ENDED 30 SEPTEMBER 2015

Mark Kimberley, Corporate Director, introduced a report, which had been circulated prior to the meeting, informing Members of the performance monitoring of the 2015/16 Prudential Code Indicators, and advising Members of the quarterly treasury activity, as required by the Treasury Management Strategy.

RESOLVED:

To note the report, together with the Treasury Activity Report for Quarter 2 at Appendix 1 to the report, and the Prudential and Treasury Indicator Monitoring for Quarter 2 at Appendix 3 to the report.

50 PROGRESS REPORTS FROM PORTFOLIO HOLDERS.

Councillor Peter Barnes (Environment)

- Fly tipping remains an unwelcome problem across the Borough.

- Extra car parking and areas of hard standing were now on place at Gedling Country Park.

- Plans for Christmas lighting across the area were in place.

- Improvement works to the Front Street area were underway.

Councillor Henry Wheeler (Housing, Health and Well-being)

- Accreditation to make Gedling Borough Council sites breast feeding friendly would be possible shortly.

- It was hoped to put in place a ban on mixed martial arts sessions taking place in the Borough due to concerns about safety.

- A meeting had taken place with the Department for Work and Pensions, Gedling Homes and the Revenues and Benefits Team to discuss the impact of welfare reforms.

- There had worryingly been a recent increase of 55% in demand for homelessness services.

- Gedling Homes had been forced to make 13 compulsory redundancies due to budget cuts.

Councillor David Ellis (Public Protection)

- There continued to be a downward trend in reported crime and anti-social behaviour across the Borough.

- A recent conference on serious and organised crime highlighted the significance of hidden crime such as human trafficking.

- Options for future policing in Carlton in light of the closure of the area's police station were recently discussed.

- Details of enforcement action taken by the Public Protection team were highlighted in a report to the Environment and Licensing Committee and it was hoped to share this information more widely to Councillors.

- CCTV contracts for the new cameras in Calverton had been completed and would soon be operational.

Councillor Jenny Hollingsworth (Growth and Regeneration)

- Laura Webb had been appointed as the YOUNG project intern in Economic Development and would be engaging with 14-21 year olds to promote work experience opportunities.

- The consultation on the proposed development at Top Wighay closed and a report will be presented to Cabinet.

- A bid had been made to build 8 starter homes in Netherfield.

- A report on options for Carlton and Arnold Town Centres has been prepared.

- A recent visit to Larkhill Retirement Village has taken place which demonstrated some interesting ideas that could be applied in the future Gedling schemes.

- A conference on town centre development was recently attended and proved useful.

Councillor Kathryn Fox (Community Development)

- A recent Halloween crafts event had taken place and was very popular.

- There would be a Christmas arts and craft event at the Civic Centre on 28 November including activities for children with special educational needs and Christmas tree lights switch on by the Mayor.

- The annual evolution dance festival will take place on 9 December at Carlton Academy.

- Gedling funded arts sessions would be taking place at Killisick Children’s Centre in November and December.

- The Big Window Theatre Company had been awarded funding to provide early years drama in Newstead and Killisick.

Councillor Michael Payne (Resources and Reputation)

- The results of the Gedling Conversation and residents’ satisfaction survey were currently being analysed and would be presented to Cabinet soon.

- The next issue of the Contact magazine was being presented and would be delivered soon.

- Preparations for next year’s budget setting were ongoing and the council awaits the announcement of the Comprehensive Spending Review and subsequent finance settlement from the government.

Councillor John Clarke (Leader of the Council)

- The Chief Executive updated Cabinet about the plans for accommodating refugees across Nottingham and Nottinghamshire. He said that there were plans underway to accommodate 100 refugees across the County and City areas with the majority placed in the City due to the better support networks that were available. He added that members would be kept informed at all stages and that it was anticipated a small number of refugees would be accommodated in the Borough before the end of the year.

51 MEMBER'S QUESTIONS TO PORTFOLIO HOLDERS.

None.

52 ANY OTHER ITEMS THE CHAIR CONSIDERS URGENT.

None.

The meeting finished at 4.00 pm

Signed by Chair:
Date:

Agenda Item 4

Gedling Borough Council

Report to Cabinet

Subject: Retaliatory Eviction and the Deregulation Act 2015

Date: 17 December 2015

Author: Food, Health, and Housing Manager

Wards Affected

Borough wide

Purpose

To brief Cabinet on new legislation to protect private rented tenants against "retaliatory eviction" where they have a legitimate complaint about the condition of their property. The legislation also brings in some additional housing related requirements for landlords which are detailed in this report.

Key Decision

This is not a key decision.

Background

Retaliatory eviction (introduced by the Deregulations Act 2015) is where a tenant makes a legitimate complaint to their landlord about the condition of their property and, in response, instead of making the repair their landlord retaliates by serving them with an eviction notice.

The Department of Communities and Local Government guidance identifies retaliatory eviction (see background paper 1 of this report) as unacceptable practice and states that no tenant should fear becoming homeless because they have asked for a necessary repair.

A tenancy is an agreement between landlord and a tenant. It is a contract that allows each of them certain rights, and also requires them to fulfil certain responsibilities. The majority of tenancies in private rented accommodation are known as assured shorthold tenancies. These usually last for 6 or 12 months, although if the landlord and tenant agree, they can be for longer.

The Deregulation Act 2015 applies to all new assured shorthold tenancies that start on or after 1st October 2015. In practice, this means that they will apply to almost all tenancies entered into with a private landlord on or after this date.

The new provisions apply where a tenant makes a genuine complaint about the condition of their property that has not been addressed by their landlord, their complaint has been verified by a local authority inspection, and the local authority has served either an improvement notice or a notice of emergency remedial action. Once the Authority has served one of these notices a landlord cannot evict that tenant for 6 months using the no-fault section 21 procedure. The landlord is also required to ensure that the repairs are completed.

The Department for Communities and Local Government guidance advises that tenants should always report any disrepair or poor conditions that may arise to the landlord as soon as possible. They should put their complaint in writing. This is consistent with the Council's housing disrepair complaints procedure. In order to rely on the protection against retaliatory eviction a tenant must approach the landlord in the first instance.

If, after 14 days from the tenant making the complaint, the landlord does not reply, or they do but that reply is inadequate, or they respond by issuing a section 21 eviction notice, the tenant should approach the local authority and ask them to inspect the property and verify the need for a repair.

Officers from the Food, Health and Housing Team will arrange to inspect the property in accordance with the Housing Act 2004. If the inspection verifies the tenant's complaint, we will take appropriate action. There are a number of possible enforcement options including improvement notices and notices of emergency remedial action. The guidance and the Council's enforcement policy both encourage the Council to always engage with the landlord first, in order to try and resolve the problem informally. If the Council serves and Improvement Notice or a Notice of Emergency Remedial Action, the landlord cannot evict the tenant for 6 months using the no-fault section 21 eviction procedure.

Additional requirements for a new tenancy that begins on or after 1st October 2015

Together with the retaliatory eviction protection the Government has introduced some additional requirements for landlords. At the start of a new tenancy, the landlord should provide a tenant with certain documents, these include the following:

- A valid Energy Performance Certificate. An Energy Performance Certficate (EPC) contains information about how much it will cost to heat the property. It also offers recommendations about how to reduce energy costs and save money.
- A valid annual Gas Safety Certificate (where they have a relevant gas

appliance). A Gas Safety Certificate is proof that the gas appliance has been checked by Gas Safe registered engineer. Each appliance must be checked and certified each year.

- A copy of the Government's Department for Communities and Local Government, "How to rent: the checklist for renting in England" guide. This can be in electronic pdf format if the tenant has supplied an email address, otherwise the tenant should be supplied with a paper copy. The guide gives tenants key details about their rights, and what they should expect from private renting. It also gives information about what to do if there is a problem during the tenancy. The guide is free from the Department for Communities and Local Government website.

If the landlord does not supply these documents at the start of each new tenancy from 1st October 2015, they should be supplied as soon as possible thereafter. If these documents have not been supplied, the landlord cannot serve a section 21 notice.

The changes introduced by the Deregulation Act 2015 also make it more straightforward for landlords to evict a tenant where they are allowed to do so. The Department of Communities and Local Government have produced a new form that landlords must use when they want to evict a tenant where the tenant has not breached their tenancy agreement (referred to as a 'no fault' or 'section 21' eviction)

Proposal

It is requested that Members note the new provisions to prevent retaliatory eviction introduced by the Deregulation Act 2015.

Alternative Options

This report is to brief Members on new powers there are no alternative options proposed.

Financial Implications

The legislation does not directly impose any requirements on the Council but Officers may come under increased pressure to exercise enforcement against landlords in order to protect tenants from eviction.

The Government's guidance and Council's enforcement policy both propose informal action in the first instance where complaints are received followed by enforcement where conditions are not improved – this does not differ from the current approach adopted by officers.

It is anticipated that any additional demand on the Council will be delivered within existing resources.

Appendices

None.

Background Papers

1. Retaliatory Eviction and the Deregulation Act 2015 – A guidance note on the changes coming into force on 1 October 2015 - issued by the Department for Communities and Local Government.

2. Department for Communities and Local Government, “How to rent: the checklist for renting in England” guide

Recommendation

That Members note the new provisions introduced by the Retaliatory Eviction and the Deregulation Act 2015.

Reasons for Recommendations

To make Members aware of the new provisions.

Gedling Borough Council

Report to Cabinet

Subject: The Smoke and Carbon Monoxide Alarm (England) Regulations 2015 – statement of principles for determining financial penalties

Date: 17 December 2015

Author: Food, Health, and Housing Manager

Wards Affected

Borough wide

Purpose

1) To brief Cabinet on new legislation imposing requirements on landlords with respect to to smoke alarms and carbon monoxide alarms.
2) To brief Cabinet on the 'Statement of Principles' prepared in accordance with regulation 13 of the Smoke and Carbon Monoxide Alarm (England) Regulations 2015 ("the Regulations") that has been adopted by the Portfolio Holder for Public Protection.

Key Decision

This is not a key decision

Background

The Regulations came into force on 1st October 2015. Private sector landlords from 1st October 2015 are required to ensure that at least one smoke alarm is installed on every storey of their rented property and that a carbon monoxide alarm is installed in any room containing a solid fuel burning appliance. The Regulations also require landlords to ensure that such alarms are in proper working order at the start of each new tenancy.

The requirements of the Regulations will be enforced by the Local Authority. Local Authorities are required to issue a remedial notice where they have reasonable grounds to believe a landlord has not complied with one or more of the requirements. The landlord must comply with the remedial notice within 28 days of service. If they do not, the Local Authority must carry out the remedial action to ensure the requirements in the Regulations are met and may issue a civil penalty charge of up to £5,000 to the Landlord. The civil penalty charge is the only way the Council can recover any costs incurred from enforcing the legislation, the Council cannot prosecute the landlord for non-compliance with the remedial action notice. Regulation 13 requires the Authority to prepare and publish a statement of principles which it proposes to follow in determining the amount of a penalty charge.

Appendix A shows the ‘Statement of Principles’ October 2015 that has been approved by the Portfolio Holder for Public Protection.

The financial penalty charge for non-compliance with a remedial notice will be £1,000 for a first offence. With an early payment discount of 25% making it £750 if paid within 14days beginning on the day on which the penalty charge notice was served.

For subsequent breaches of duty to comply with a remedial notice by the same landlord the penalty will be £5,000 to deter continued non-compliance and an early payment will attract a discount of 50% making it £2,500.

Proposal

It is requested that Members note the new provisions to protect the health and safety of tenants and the approved ‘Statement of Principles’ October 2015.

Alternative Options

This report is to brief Members on new provisions, there are no alternative options proposed.

Financial Implications

These regulations place additional duties and powers on Local Authorities, it is considered these will be delivered within the existing resources available to the Council. When carrying out remedial action in accordance with the legislation costs will be incurred which will include; officer time, materials, and the cost of the actual works. These costs can only be recovered through the financial penalty charge, it is considered the proposed charges will cover the costs incurred by the Council and contain a punitive element to penalise the landlord for non-compliance.

It not considered that a significant amount of landlords will receive a penalty charge as many will already be compliant. Those who are not compliant will be issued a notice requiring them to install the detectors within 28 days before the works would be carried out by the Council and the penalty charge issued.

Appendices

Appendix A – Statement of Principles, October 2015

Background Papers

The Smoke and Carbon Monoxide Alarm (England) Regulations 2015 – Explanatory Booklet for Local Authorities

Recommendation

That Members note the new provisions introduced by the Smoke and Carbon Monoxide Alarm (England) Regulations 2015 and the adopted 'Statement of Principles' October 2015.

Reasons for Recommendations

To make Members aware of the new provisions.

This page is intentionally left blank

Gedling Borough Council

The Smoke and Carbon Monoxide Alarm (England) Regulations 2015

Statement of principles for determining financial penalties

Serving People Improving Lives

October 2015

1.0 The purpose of this statement of principles for determining financial penalties

1.1 This statement sets out the principles that Gedling Borough Council ("the Authority") will apply in determining the amount of penalty charge payable by a landlord when that landlord breaches their duties as set out in The Smoke and Carbon Monoxide, Alarm (England) Regulations 2015 ("the Regulations").

2.0 The legal framework

2.1 The Regulations introduce the following requirements for all landlords during any period beginning on or after 1st October 2015 when the premises are occupied under the tenancy—

(i) a smoke alarm is equipped on each storey of the premises on which there is a room used wholly or partly as living accommodation;

(ii) a carbon monoxide alarm is equipped in any room of the premises which is used wholly or partly as living accommodation and contains a solid fuel burning combustion appliance; and

(iii) checks are made by or on behalf of the landlord to ensure that each prescribed alarm is in proper working order on the day the tenancy begins if it is a new tenancy

2.2 Where the Authority has reasonable grounds to believe that:

- There are no or insufficient number of smoke alarms or carbon monoxide detectors in the property as required by the Regulations or;
- The smoke alarms or carbon monoxide detectors were not working at the start of a tenancy or licence;

Then the Authority shall serve on the Landlord in a method prescribed by the Regulations, a remedial notice ("the notice") detailing the actions the landlord must take to comply with the Regulations, such action to be taken within 28 days from the date the notice is served.

2.3 Where the Authority are satisfied on the balance of probabilities that a landlord on whom a remedial notice has been served has failed to comply with the notice the Authority must undertake the remedial action specified in the notice.

2.4 Regulation 8 provides that the Authority may require the landlord to pay a penalty charge if the Authority is satisfied on the balance of probabilities that the landlord on whom it has served a remedial notice under regulation 5 has failed to take the remedial action specified in the notice within the period specified. The penalty charge is payable within 28 days of the penalty charge notice being served on the landlord.

3.0 The scope of this document

3.1 Regulation 13 requires the Authority to prepare and publish a statement of principles which it proposes to follow in determining the amount of a penalty charge.

3.2 The Authority may revise its statement of principles and, where it does so, it must publish the revised statement.

3.3 Where a penalty charge is made, the Authority must have regard to the statement of principles published and in place at the time when the breach in question occurred, when determining the amount of the penalty charge.

3.4 In particular the Authority will have regard to satisfying the balance of probabilities that the landlord has failed to take the remedial action required in the notice.

3.5 This document sets out the principles which Gedling Borough Council will apply and will have regard to when exercising its powers under Regulation 8.

4.0 The purpose of imposing a financial penalty

4.1 The primary purpose of the Council's exercise of its regulatory powers is to protect the interests of the public, although they will also have a punitive effect. The primary aims of financial penalties will be to:

- change the behaviour of the landlord.
- eliminate any financial gain or benefit from non-compliance with the regulations.
- be proportionate to the nature of the breach of the regulations and the potential harm outcomes.
- aim to deter future non-compliance.
- reimburse the costs incurred by the Authority in undertaking work in default

5.0 Criteria for the imposition of a financial penalty

5.1 The Authority will need to be satisfied on the balance of probabilities that the landlord on whom a remedial notice has been served has failed to take the remedial action specified in the notice, only then can a financial penalty be issued.

5.2 In deciding whether it would be appropriate to impose a penalty, the Authority will take full account of the particular evidence, facts and circumstances of the breach under consideration.

6.0 Principles for determining the amount of a financial penalty

6.1 Regulation 8(2) states the amount of the penalty charge must not exceed £5,000. The penalty charge comprises two parts:

1) a punitive element for failure to comply with the absolute requirement to comply with a remedial notice (subject to any representation made by a landlord to the Authority) and
2) a cost element relating to the works carried out by the Authority.

6.2 It is important that landlord's understand the importance of installing and maintaining the correct alarms to ensure their tenants' safety. The punitive element of the penalty aims to hold those landlords who breach the regulations to account and ensure that the duties are taken seriously for the protection of tenants.

6.3 There is no other provision made in the regulations for enforcement authorities to redeem costs for any remedial work which they are required to carry out when a landlord fails to comply with a remedial notice. The collection of the financial penalty is the only method by which any recovery pf the costs of the remedial works can be recovered. The level of remedial works required will vary depending on the circumstances of each case. For clarity, the Authority have set a fixed rate for its penalty charges which aims to recover all costs incurred with remedial works including officer time, materials and cost of actual works, together with a punitive element to deter landlords from non-compliance. The penalty charge is the only opportunity for the Council to penalise the landlord for non-compliance or recover associated costs.

6.4 The period within which the penalty charge is payable is 28 days beginning with the day on which the penalty charge notice is served.

6.5 Regulation 9 (2) states that if a landlord pays the penalty charge within 14 days beginning with the day on which the penalty charge notice is served, the penalty charge will be reduced by an amount specified in the notice.

6.6 The Authority may also review the penalty charge if the landlord serves a notice on the local housing authority requesting a review.

6.7 The Authority will, in accordance with the legislation reduce the penalty charge in relation to payment within a specified "early payment" period. The specified period for early payment is within 14 days beginning with the day on which the penalty charge notice was served.

6.8 For a first offence the fine applied will be £1,000 and an early payment will attract a discount of 25% making it £750.

6.9 For subsequent breaches of duty to comply with a remedial notice by the same landlord, the penalty will be £5,000 to deter continued non-compliance and an early payment will attract a discount of 50% making it £2,500.

7.0 Procedural matters

7.1 The regulations impose a number of procedural steps which must be taken before the Authority can impose a financial penalty. Before imposing a requirement on a landlord to pay a penalty charge the Authority must, within a period of six weeks from the point at which it is satisfied that the landlord has failed to comply with the requirements of the remedial notice, serve a penalty charge notice setting-out**:**

- the reasons for imposing the penalty charge;
- the premises to which the penalty charge relates;
- the number and type of prescribed alarms (if any) which an authorised person has installed at the premises;
- the amount of the penalty charge;
- that the landlord is required, within a period specified in the notice—
  (i) to pay the penalty charge, or
  (ii) to give written notice to the local housing authority that the landlord wishes the authority to review the penalty charge notice;
- how payment of the penalty charge must be made; and
- the person to whom, and the address (including if appropriate any email address) at which, a notice requesting a review may be sent and to which any representations relating to the review may be addressed.

7.2 A penalty charge notice must be paid within 28 days beginning with the day on which the notice is served, unless the Authority receives written notice from the landlord that they wish the Authority to review the penalty charge notice. However if the payment of the penalty charge is made within 14 days beginning with the day on which the penalty notice is served, the penalty charge will be reduced by an amount specified in the notice.

8.0 Review of penalty charge notice

8.1 In accordance with the provisions of Regulation 10 the Authority will on receipt of a written notice requesting a review from the landlord consider any representations made by the landlord, and serve notice of its decision whether to confirm, vary or withdraw the penalty charge to the landlord. Any such written notice must be received by the Authority not less than 28 days after the day on which the penalty charge notice is served.

8.2 In conducting the review, the Authority will consider any representations made by the landlord, and serve notice of its decision whether to confirm, vary or withdraw the penalty charge to the landlord.

8.3 A landlord who, having requested a review of a penalty charge notice, is served with a notice confirming or varying the penalty charge may appeal to the First-tier Tribunal against the Council's decision. The grounds for appeal are set out in Regulation 11(2) and can also be found on the back of the penalty charge notice.

9.0 Remedial Action

9.1 It is the decision of this authority that the smoke alarms to be fitted within the premises where remedial action is undertaken are to be battery smoke alarms. However, these are to be tamper-resistant alarms with a minimum ten year battery life.

9.2 Where the penalty charge is not paid the Authority may recover the penalty charge on the order of a court, as if payable under a court order.

Agenda Item 6

Report to Cabinet

Subject: **Update to the Information Security Policy**

Date: 17 December 2015

Author: Research and Development Manager, ICT Support and Council Solicitor & Monitoring Officer

Wards Affected

Not applicable.

Purpose

To seek approval for changes to the Information Security Policy and request delegated powers to approve minor updates or any changes required in order to secure PSN compliance (or equivalent security standard).

Key Decision

This is not a Key Decision.

Background

1.1 Members will recall that the Council's Information Security Policy which was created by the Data Security Group in 2012 and approved by Cabinet 4 April 2013. Members will be aware that the Policy sets out the legal framework for information security along with clearly defined responsibilities. It also includes arrangements for the following:

- Access Controls
- Remote working
- Mobile devices
- Procurement of Systems
- Secure Disposal
- Protective Marking
- Managing security incidents

1.2 The Data Security Group has reviewed the current policy to ensure that it is fit for purpose and has concluded that updates to the Policy are required to meet the continual need to adequately protect the Council's information assets and ensure continued compliance with current guidance/standards.

Proposal

2.1 It is proposed that Cabinet approve the revised version of the Information Security Policy at Appendix 1 to this report. The proposed changes to the Policy fall into 3 categories:

(i) technical changes required in order to maintain Public Services Network (PSN) and Payment Card Industry Data Security Standard (PCI DSS) compliance and reflect current security guidance/standards;

(ii) a re-draft of the Data Management section in order to reflect the revised Government Security Classifications; and

(iii) minor changes to job titles and correction drafting errors.

2.2 In summary the main changes are:

Technical changes

- Expansion of the Payment Card Industry Data Security Standard (PCI DSS) section to include guidance on card handling, Point of Sale terminal configuration and inspection.
- An additional section on Wireless Networking, configuration and use to meet the Payment Card Industry Data Security Standard.
- Changed references to Government Connect to its new name of Public Services Network.
- An addition requirement for Two Factor Authentication for Web Mail access to ensure Public Services Network (PSN) compliance.
- Smartphones and tablets will allow ten attempts to enter the correct User ID and password before wiping the device instead of five, which will increase usability but maintain an appropriate level of security.

Data Management

The current Data Management section classifies the Council's information in 3 categories – Restricted, Protected and Unclassified. These were based on the National Protective Marking Scheme as set out in the Central Government Manual of Protective Security. Since the Information Security Policy was approved, these national classifications have been replaced by the new Government Security Classifications Policy. The Data Management section of the Information Security Policy has therefore been re-written to reflect this as follows:

- All Council information will be classified as OFFICIAL and the previous classifications, RESTRICTED, PROTECTED and UNCLASSIFIED no longer apply,

- There is no requirement to explicitly mark OFFICIAL information, so the previous requirement to mark all information no longer applies,

- OFFICIAL information which is particularly sensitive will be treated as OFFICIAL – SENSITIVE information to denote that it needs additional controls,

- OFFICIAL – SENSITIVE information must be clearly marked to indicate the need for those additional controls,

- The guidance on handling information has been updated to reflect the new classification,

- Special instructions for handing personal data (which is classified as OFFICIAL information) are included to ensure compliance with the Data Protection Act.

2.3 It is also proposed that Cabinet delegate authority to approve regular minor updates to the Information Security Policy or any changes required in order to secure PSN compliance (or equivalent security standard) to the Corporate Director. This will enable Officers to react quickly and ensure the Policy continues to provide a robust framework to protect the Council and the information it holds. Other changes would require Member approval.

Alternative Options

3.1 Not to approve the changes proposed, but this will result in the Policy being out of date and not complying with current guidance/standards.

3.2 Not to give a delegation to the Corporate Director, but this will mean that minor changes to Policy will require member approval.

Financial Implications

4.1 Any costs associated with the implementation of the Policy will be met within existing budgets.

4.2 Compliance with the Payment Card Industry Data Security Standard will ensure that the Council avoids additional fees by Card Processing companies in the region of £5,000 per annum.

4.3 Failure to comply with information governance legislation could result in the Information Commissioner imposing a monetary penalty of up to £500,000.

Appendices

5 Appendix 1 – Information Security Policy v1.5.

Background Papers

6 None identified.

Recommendation

THAT:

(a) The revised Information Security Policy at Appendix 1 to the report be approved; and

(b) The Corporate Director be authorised to approve future minor updates to the Policy or any changes required in order to secure PSN compliance (or equivalent security standard).

Reasons for Recommendations

7.1 To ensure that the Council has a robust up to date policy in place which protects the Council and the information it holds by providing a clear framework for preventing, monitoring and responding to information security breaches.

7.2 To allow ongoing minor updates to the policy to be made by Officers and communicated to all staff as quickly as possible.

Gedling Borough Council

Information Security Policy

Policy Statement

Gedling Borough Council has a large, and on-going, investment in Information and Communication Technology. Information security protects that investment from a wide range of threats.

The Policy was formulated by giving due regard to: -

- Risk Assessment
- Legal/statutory/regulatory requirements
- Organisational principles
- Computer Misuse Act – computer fraud, hacking, data security
- Data Protection Act

The objectives of this Policy are as follows: -

- To ensure that the Council's ICT assets - hardware, software, data and the network infrastructure - are protected against theft, loss, damage, corruption and any unauthorised actions.

- To ensure that all employees of the Council are aware of the risks to which ICT systems may be subjected and of their responsibilities to minimise those risks.

- To ensure that the Council complies with the many and varied laws surrounding Information and communications.

This Policy applies to **everyone** who has access to the Council's ICT assets, including all employees, Councillors, temporary staff including those on work experience, outside contractors and partners using the Council's equipment.

This Policy will apply whenever users are using the Council's systems, whether it is in the Council offices, working remotely from another location or at another Council's offices.

Misuse by staff will cause the matter to be considered under the Council's Disciplinary Procedure and may, in some cases, result in dismissal – particularly if a failure to comply with the Policy is deemed to be deliberate or malicious.
Misuse by Councillors may amount to a breach of the Code of Conduct and could lead to a complaint to the Standards Committee, particularly if a failure to comply is deemed to be deliberate or malicious.

Breaches of security or inappropriate use of systems must be reported to the ICT Research and Development Manager.

Violations of security procedures established within this policy will be dealt with in accordance with the Information Security Incident Management section.

Responsibilities

The Council uses Computer Systems to store and process data in order to deliver its Services. Formal 'Ownership' is vested with specific post holders across the Council. **System Owners** have responsibilities which include ensuring that the Systems they are responsible for deliver the required solutions, maintain integrity of any data held and that only authorised access is granted.

Members of the Corporate **Data Security Group** are The Council's Senior Solicitor and Monitoring Officer (Chair); Service Manager (Customer Services and IT) and Service Manager (Audit and Risk Management). The overarching remit of the group is assist the Council to fulfil its obligations to appropriately protect paper and electronic 'data' and to ensure that everyone who has authorised access to 'data' is aware of their 'data handling' responsibilities.

All staff shall ensure that they read and agree to the **Personal Data Security Commitment**, which is a companion document to this Policy.

Additionally:

The **Senior Leadership Team** shall:

- Acknowledge their overarching responsibilities for information security;
- Demonstrate commitment to the security agenda;
- Assign security responsibilities to relevant staff members
- Security roles and responsibilities are included in appropriate job definitions
- All references (including formal vetting where appropriate) are checked prior to a member of staff's commencement of employment. [Particular checks must be made on Agency staff who will be given access to the Council's Information Systems]

The **Data Security Group** shall:

- Conduct investigations into any alleged computer or network security compromises, incidents, or problems;
- Provide security guidance to Staff and independent system owners;
- Investigate aspects of violations of security policy and standards, and reporting to the appropriate Data Security Group;
- Conduct the annual Information Security Policy review and update; and
- Promote security awareness across the Council.

Also, the **Data Security Group** shall ensure that:

- Information Security training is provided to all staff within the Council, including periodic refresher training;

- All staff are promptly informed of any security issues/concerns and when this policy is updated;
- The IT Security Procedure is adhered to.
- They will discuss, resolve, maintain and monitor records of security incidents and feed back to the Senior Leadership Team (SLT) where appropriate;
- The Council's practices and procedures for the handling and transfer of personal and confidential data to ensure that they comply with statutory requirements, current government policy and recognised standards are adequate and adhered to;
- These security procedures are communicated to staff and appropriate safeguards are in place to ensure they are adhered to;
- The Council's security and policies are subject to periodic external review;
- These procedures and processes are sufficient to ensure the confidentiality of personal data, identify any weaknesses and mitigating controls; and
- Internal processes and culture where required are strengthened to achieve appropriate data security if necessary.

The **ICT Section** (referred to as "ICT") shall ensure that:

- Appropriate security controls are in place and measures undertaken to protect the Council's network and information assets;
- Staff are ONLY granted appropriate access to the Council's IT facilities in order to carry out their job;
- Third parties (such as contractors) are ONLY granted appropriate access to the Council's IT facilities in order to perform the service they have been asked to provide when authorised by the system owner;
- Network access is only granted after appropriate authorisation is received from the Line Manager and the user has formally accepted and signed up to this policy;
- Periodic network account reviews are undertaken, and any redundant accounts are promptly disabled;
- Adequate operational controls exist to ensure data protection;
- They communicate appropriate use, and consequences of misuse, to users who access the systems or data;
- Sensitive files and access control files are protected from unauthorised activity;
- LAN and workstation integrity is maintained through virus protection measures and policies;
- Day-to-day security administration is provided;
- Equipment is maintained to ensure its continued availability and integrity;
- Sufficient resources are made available to systems to ensure availability and performance;
- An inventory of all important hardware and software assets is maintained;
- Contact is maintained with relevant authorities and groups, e.g. CESG and EMWARP;
- They monitor the performance of third party services and systems, and manage changes to these contracts;
- They maintain access and audit records; and
- They create, distribute, and follow up on security violation reports.

System Owners shall:

- Act to preserve security of shared facilities, and ensure that systems they administer are operated in accordance with all applicable Information Security Standards and Policies;
- Authorise appropriate third party access (such as contractors), in order to enable them to perform the service they have been asked to provide, and inform ICT appropriately;
- Ensure that appropriate contracts are in place with supporting third party suppliers, which includes a relevant confidentiality of data clause;
- Monitor the performance of third party services and systems, and manage changes to these contracts;
- Ensure that appropriate measures are in place to prevent unauthorised access;

- Ensure that an appropriate level of access is granted to system users.

Service Managers shall:

- Ensure that staff abide by the security controls in place and measures undertaken to protect the Council's information assets;
- Provide and maintain safeguards for information systems within his/her authority, consistent with policies and standards;
- Approve appropriate data access, allowing staff to complete business-related assignments;
- Appropriately inform ICT about all staff starters, movers and leavers through the User Administration process;
- Ensure staff attend the IT security training course;
- Review, evaluate, and respond to all security violations reported against staff, and take appropriate action;
- Maintain an inventory of all electronic data systems;
- Consult ICT when procuring IT hardware and software assets;
- Inform ICT when IT hardware assets are moved between sections;
- Ensure staff have appropriate ICT training, to ensure they are able to fulfil the requirements of this policy and incidents do not occur due to lack of basic computer skills
- Security roles and responsibilities are included in appropriate job definitions
- All references (including formal vetting where appropriate) are checked prior to a member of staff's commencement of employment. [Particular checks must be made on Agency staff who will be given access to the Council's Information Systems]

The **Service Manager: Organisational Development** shall ensure that:

- Confidentiality agreements form part of the terms and conditions of employment
- The Personal Data Security Commitment Statement an integral part of the Employee Conditions of Service Policy
- The Employee Handbook refers to the latest versions of the Information Security Policy and the Personal Data Security Commitment Statement which will be kept up to date by the Data Security Group and published on the Intranet

Physical Security

Buildings Security

Buildings access for Council employees and Councillors is through the use of proximity swipe-cards at the main entrance. Employees are also required to wear ID Badges at all times, and are encouraged to challenge anyone they do not know who is not wearing a badge. Access privileges are to be revoked immediately upon an employee leaving the Council's employment. Visitors are to report to Reception, sign-in, and are to be appropriately supervised. Swipe cards must not be issued to third parties (i.e. those not employed by the Council and are not Councillors) unless they have signed a Proximity Card and Confidentiality Agreement.

The following additional steps should be taken to ensure the security of information, in the event that unauthorised people gain access to Council premises:

- Offices are not left unattended where possible during normal working hours;
- All computers in vulnerable areas (e.g. ground floor rooms) are physically secure;
- Computers are locked when users are away from desks for a short time and log off or switch off when not in use for longer, such meetings, lunchtime and going home.
- Confidential/sensitive data is not left in view when not in use, this data should be locked away;
- Laptops, mobiles devices and removable storage are not left in view when not in use.

Under no circumstances should personal/confidential/sensitive information be left in public areas or on desks unattended for any period of time. New computer installations shall not site computers in public or insecure areas unless controls are put in place to prevent theft or misuse, e.g. kiosk type devices.

Off Site Security

Care must be taken when operating Council IT equipment off-site. When travelling, care must be taken to protect portable computing devices (Laptops, PDAs, and mobile phones etc) from theft or damage. Equipment is to be carried as hand-luggage, not left unattended, and disguised where possible. When left in vehicles, equipment is to be locked in the boot and out of public view. When used at home, equipment is to be secured (e.g. logged out/locked away) when not in use and stored out of view.

When operating a Laptop or PDA in public places (e.g. on a train or in an airport), the user must be aware of any security risk presented by being observed by others (‘shoulder-surfing’).

The loss or theft of IT equipment (including mobile phones) is to be reported as a Security Incident to the ICT Helpdesk.

Paper records containing confidential or sensitive information must be kept secure when off-site in a lockable case and totally separate from valuable items such as laptops.

Computer and Networking Equipment

Network computer equipment is located in a controlled and secure environment. Critical or sensitive network equipment is housed in an environment that is monitored for temperature, humidity and power supply quality, and is protected by a secure perimeter with appropriate access restrictions. The Customer Services & IT

Manager and IT Technical Manager are responsible for the effective operation of these controls, which include but are not limited to:

- Redundant power supplies;
- Uninterruptable Power Supplies;
- Physical locks;
- Fire detection; and
- Air conditioning.
- Only authorised staff are permitted to enter server and communications rooms;
- Where kiosk type computers are required in public areas, these systems are secured such that they do not pose a threat to the main network;
- Visitors (such as consultants and engineers) are logged in and out and always escorted whilst in sensitive computer areas; and
- 3rd Party equipment shall not be connected to the Council’s network; however it may be connected the projectors in meeting rooms.

Secure Disposal or Re-use of Equipment

All electronic and data storage media disposal must be carried out by ICT. Please contact the ICT Technical Manager.

ICT must be informed as soon as possible if a device is lost or stolen.

All PCs and Laptops are replaced on a multi-year cycle by ICT. Equipment that is no longer required should have all data and licensed software removed from it before being disposed or re-deployed (as stipulated under the WEE directive) using a specialist secure disposal company. Certificates of data destruction should be obtained and kept on file.

Disposal or transfer of equipment is to be recorded in the relevant Asset Inventory. Software Asset Inventories are to be adjusted to reflect licence status as appropriate.

All disposed media or equipment will be disposed in such a way as to make the data it previously contained impossible to recover. Currently the following methods are used:

Item	Disposal Method
Computer Hard Disk	3 Pass wipe using disk cleaning software plus wipe by disposal company
CDs/DVDs etc	Shredding
Magnetic Tapes/floppy disks	Degaussing plus smelting by disposal company
Smartphones or tablets, including stolen or missing	Security wipe through interface or remote wipe
USB sticks / PDAs / Faxes / memory cards / Dictaphones / other devices	Use manufacturer approved wiping procedure, if none available see physical destruction below
Microfiche	Incineration
Items above where standard method is ineffective	Physical destruction of item by whatever means is possible. If necessary using a hammer. (Ensure PPE is used)

Disposal of Paper Documents

Documents must not be retained longer than stipulated within the Council's Document Retention and Disposal Policy.

All documents containing 'Confidential/Sensitive' information must be shredded and disposed of through the Council's confidential waste process (see Data Management).

Operations

Operational Procedures

ICT will ensure that operational procedure documents are created and maintained. End user documentation will be distributed, and sensitive documents shall be protected from unauthorised access. Systems Owners will do the same for their individual systems.

Changes to systems shall be approved either by System Owners for the individual systems, or the ICT Technical Manager for Council wide systems. Where major changes to the security environment are required the Data Security Group shall also be consulted.

Segregation and separation

All users shall run in standard user privilege, except for ICT Support staff. Access to system utilities and configuration not required by the user will be disabled.

Developers shall have administrative control over the test services, but not production systems. ICT Support staff will move systems from test to production once appropriate testing has been completed.

Back Up

ICT shall ensure all systems are regularly backed up. For live data this should be at least every working day. Backups shall be stored in a fireproof safe.

Backups shall be taken off site to a secure location at least twice a week in case the primary building is destroyed or is otherwise unavailable.

Software

It is essential that only licensed software is used, and installed by ICT staff only, on all hardware platforms owned by the Council.

All program software master media and licenses will be stored by ICT.

Deliberate unauthorised access to, copying, alteration, or interference with computer programs or data is prohibited.

Users shall contact ICT before any external party installs any software or loads any data on any of the Council's hardware platforms, in order that ICT staff can make arrangements to be available to oversee the installation and ensure that the Council's policies and strategies are adhered to. Last minute calls are not acceptable.

It is the responsibility of all employees not to use or allow unlicensed software to be operated on Council owned equipment and to report any breach of this rule to the ICT Technical Manager.

Council systems, networks and communication systems should never be used to store or distribute personally owned pictures, music, videos, photos, books or data of any kind.

No member of staff, other than members of ICT shall attempt to install or copy all or any part of any application software onto or from Council owned hardware or other media.

Screensavers may contain malware and therefore you should not use any screensavers other than the standard ones installed by ICT. Desktop themes may be customised using the Microsoft website. Employees/Councillors must not use personal photos or any backgrounds that may offend either other staff or visitors and are suitable for a work environment. Avoid dynamic themes as these may use too much Internet bandwidth. If issues arise a standard wallpaper may be enforced.

No software, whatsoever, may be downloaded from the internet without permission from ICT.

Software Patching

Not only is patch management best practice, it is also a requirement of Public Services Network and subject to annual external independent review. It is a requirement of Public Services Network that un-patchable software must not be used on a site with a GCSx Connection. Software with a known security issue, that cannot be patched must be replaced or discontinued.

The following Patch Management Policy applies to all systems and servers within the Council.

There are 3 levels of patch management within the Council:

- Microsoft product patches;
- System owner software patches;
- Non-Microsoft product patches.

All patches will be authorised by the ICT Senior Technical Officer and tested prior to being applied to the Council's systems. Patch testing should always be performed on a limited number of workstations before authorisation can be given to apply the patch in the live environment. The extent of testing will vary depending on the severity of the patch; however it will be as full and practical as possible, particularly where a large number of workstations or corporate databases are involved.

Responsibilities

The Council's ICT Section will be predominantly responsible for the testing and application of security patches. Users must inform the ICT Service Desk if the application of a patch affects the configuration and normal operation of their desktop or laptop.

All staff shall ensure that:

- They login to the Council's PC on a regular basis and ensure all updates are applied. This is especially import for mobile devices;

- They notify the ICT Service Desk, ext 3888, of any desktops and laptops in their work areas which are not used on a frequent basis or logged onto the network;

- They are vigilant of any changes to the normal operation of their desktop / laptop following the application of any patches and notify the ICT Service Desk, ext 3888 of any such changes.

The **ICT Section** shall ensure that:

- Appropriate security controls are in place and measures undertaken to protect the Council's systems and services from the risk of failure;

- Where appropriate, additional system backups are performed prior to applying a patch;

- Where applicable, systems are cloned and satisfactorily prepared for patching;

- Where necessary, additional testing is carried out in accordance with notes provided by the system suppliers;

- Prior to applying a patch to the live environment, pre-configuration, post-configuration and recovery are tested first;

- A fully referenced file is maintained of major system patches and accompanying notes and all patches are signed off once applied.

The **System Owners** shall ensure that:

- They follow change control procedures for the application of system patches and log a call with the ICT Service Desk;

- Patches are applied at a mutually agreed time with ICT;

- ICT are notified in sufficient time of the purpose of all system patches as they may affect the security infrastructure and test data may be required;

- Any infrastructure requirements are formally noted and an impact assessment is undertaken;

- Assurance is sought from system suppliers to confirm all modules affected by a patch have been tested prior to release;

- A backup of the system is made prior to applying a patch and a fall back plan is agreed;

- All users have logged out of the system prior to a patch being applied;

- They thoroughly test and sign off the release before it is made live;

- System procedures are updated where necessary following the application of a patch.

Windows Patching

Windows patches are checked by the ICT Senior Technical Officer. The list of patches are reviewed and approved for testing initially, prior to authorising them for release to live workstations on the network.

Users will notice that their desktop or laptop may take a few minutes longer to load following the application of patches.

All relevant new security patches will be installed within one month of release.

Application Patching

The application of system patches to the live environment will require users to log out of the system affected. Notice will be given accordingly by the System Owner and ICT. This process is managed by System Owners or supplier in conjunction with ICT upon the notification of a patch by the system suppliers.

Software Patching

Recognised trusted websites are checked monthly to ensure any new vulnerability or security patches are identified in a timely manner. Once approved the fixes are then applied within one month of release.

Anti Virus Definition Updates

The software provider automates scheduled downloads of virus definitions every hour. Client roll outs are controlled by the software and are rolled out automatically as soon as they are switched on.

Software Development

All software, other than purchases from external suppliers, shall be developed by ICT. Source code for all software shall be protected from unauthorised access.

It is possible to create quite elaborate programs and systems using the Office Suite, particularly in Access, but also Word, Excel and Outlook. The Council strongly discourages this due to the inherent complexity of software development and the lack of skills within departments to support these applications if the developer leaves the Council. ICT cannot take responsibility for, or reverse engineer, any departmentally developed applications. Should any existing application be business critical and require this kind of attention it will be the responsibility of the department to pay for external specialist assistance.

Should any employee/Councillor have a software requirement please contact ICT to discuss possible solutions.

Email / Internet

The Council's Internet services are primarily for business use. Personal internet use is only allowed in the employee's own time, with the manager's permission, and should not interfere with an employee's work or that of colleagues. Internet usage may be monitored and any personal use considered excessive will be reported to managers. Managers may also request reports of employees they have concerns about.

The Council operates software which blocks sites which are not considered to be of a work nature e.g. hate speech, pornography, hacking etc. This is to protect the use of the Council's reputation, and bandwidth, which is not only used for work purposes but for customers to access the Council's website.

The Council not only owns the hardware and software but also e-mails and any downloaded web pages.

The Council may inspect e-mails (including personal e-mail) at any time without notice, for the following reasons: -

- Criminal activity;
- A breach of council policy/protocol;
- Operational reasons for example arising from employee absence;
- Fault finding by ICT due to a helpdesk call.

Approval for access to an email account for operational reasons may be given by the relevant line manager or Service Manager. Approval for access to an email account for fault finding reasons may be given by the Service Manager: Customer Services & IT.

In all other circumstances approval must be given by the Monitoring Officer or Service Manager: Audit and Risk Management. This approval should be in writing and include: -

- The reason for the request;
- The name of the individual; and
- If possible the e-mail subject matter or suspected files or further details.

It is the user's responsibility to manage their e-mails.

Where an employee is liable to be absent from work for long periods, provision should be made by the employee to ensure that work related e-mails could be disseminated to appropriate officers.

Remember e-mail messages may have to be disclosed in litigation or in response to an information request under FOI, therefore be polite and courteous.

Obtain confirmation of receipt for important e-mails sent.

ICT will ensure incoming and outgoing e-mails are virus checked.

Do not deliberately visit, view or download any material from any web site containing sexual or illegal material or material that is offensive in any way whatsoever.

Users who accidentally visit or view an unsuitable site **must** inform ICT in order that the site can be blocked to protect the other users.

All Internet sites visited are logged; this information is available to management and Internal Audit who can use it to ensure the legitimacy of sites visited*.*

Since most information sent over the Internet is not secure, consideration must be given to the nature of the content. If the message contains sensitive information, alternative transmission methods or encryption should be considered. (See Classification/Categorisation of Information Assets for further guidance).

Each individual accessing the Internet **must** be logged onto the PC as themselves.

E-Mail

Unauthorised or careless use of Email may present a legal risk to the Council or individual members of staff.

Users Responsibilities

It is the user’s responsibility to save important emails externally from the e-mail system e.g. in directories on the servers.

E-mails should be formatted in the following way:

1. Ensure the recipient address is correct, especially where the email system suggests or remembers addresses;
2. Always enter an appropriate subject;
3. Begin the message with the name of the person the email is being sent to;
4. The message should follow the guidelines over content (below);
5. Unless absolutely necessary, do not include graphics in e-mails;
6. Ensure that e-mail attachment sizes are kept to a minimum. Many systems will not accept emails greater than 10MB and emails expand due to the way they have to be transmitted, so there is no guarantee large attachments will be received;
6. All email fonts must be set to arial 12 and all written text should be in black to comply with guidance from the Royal National Institute for the Blind (RNIB);
7. An email signature must be set up by all users which conforms to the Council’s Style Guide, see example below:

Firstname Surname
Job Title

Gedling Borough Council
Civic Centre, Arnot Hill Park
Arnold, Nottingham NG5 6LU
Telephone number / Mobile number
www.gedling.gov.uk

For the latest news and events, follow us on Twitter @GedlingBC or like us on Facebook

8. Electronic signatures must not be used in emails as these can be used by others for fraudulent purposes;
9. Corporate strap lines must not be used unless approved by the Service Manager: Communications as they would cause a large increase in storage requirements for e-mails. Service specific strap lines can only be used if approved by the relevant Service Manager;
10. Backgrounds and pictures must not be used as they would cause a large increase in storage requirements for e-mails;

11. An out of office message should be used when staff are not contactable for at least one working day, and should contain the following details as a minimum:

    When the member of staff will next be available and the name and email address of at least one other officer to be contacted if the matter is urgent;

12. Do not send e-mail attachments when a link to the document can be made to save on storage usage.

E-mail content guidelines

Always remember, an e-mail is **not** an informal communication. It has the same authority as any other communication from and within the organisation, such as a letter or telephone call. In the same way as a letter, its contents can be used in a court of law.

As a basic rule, if the information wouldn't be put in a letter, don't put it in an e-mail.

E-mails are not confidential or automatically encrypted.

An e-mail attachment containing sensitive data should be transmitted in one of the following ways:

> If the recipient is a government body, the Public Services Network Secure Extranet (Gcsx) e-mail should be used with a Gcsx e-mail address as the recipient and the sender must use a Gcsx user account to send the e-mail, attachments cannot be encrypted using this facility.
>
> Other than the above the attachment must be encrypted, passwords must be sent to the recipient using a different method e.g. phone. Passwords must never be sent in the same email as the attachment.

Mailboxes are owned by the Council and are not the personal property of staff members.

Staff should be aware of who has access to their mailbox and review this regularly, especially during periods of re-organisation. Make sure access is not granted to the "Default" or "Anonymous" roles.

If it is suspected that there is a case of misuse or abuse, the contents of e-mails can be examined and may be used as evidence in disciplinary cases.

It is also important to remember the implications of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 under which information contained in e-mails can be requested. In addition a Subject Access Request under the Data Protection Act 1998 would entitle anyone to see all e-mails which contain data relating to them.

E-mails sent must not contain or have as attachments any of the following:

1. Copyrighted material, such as MP3, video, eBooks, mapping or software;
2. Offensive material;
3. Phishing emails, such as fraudulent requests for bank or logon details;
4. Moving graphics;
5. Music;

6. Pictures unless work related or approved by senior management;
7. Chain letters; and/or
8. Jokes.

Breaches of the above will be considered as a misuse or abuse and could lead to disciplinary proceedings.

E-mails received which fall into categories 1 and 2 above must be reported to your Manager.

Watch the wording

Take all due care in the way e-mails are worded. Especially be aware that:

1. Binding contracts may be inadvertently created by careless wording;
2. Defamation of colleagues or other parties within an e-mail must not occur and care should be taken to ensure that this does not happen accidentally. Staff must specifically avoid expressing opinions about individuals;
3. Inappropriate reference to race, colour, ethnic origin, nationality, gender, sexual orientation, religion, marital status, disability or age is unacceptable;
4. The use of abrupt and inappropriate language can create a bullying tone and possible offence or even harassment to others; and
5. The use of UPPER CASE letters for a complete word, sentence, paragraph or complete e-mail can be interpreted as shouting and should not be used.

E-Mail systems

The only e-mail facility which can be used on the Council's equipment is the Council provided e-mail system. The use of external e-mail provision is forbidden with the exceptions of the use of external accounts for non-networked equipment (Laptops with remote access capability are regarded as networked equipment) installed by ICT, and for Councillor's personal accounts.

The Council has implemented Outlook Web Access (OWA) which enables staff and Councillors to access their e-mails from a non-Council owned device. This facility should only be used with the Manager's approval. Ensure this is only used on devices with no virus or other malware installed.

Automatic forwarding of emails to external email addresses is prohibited as confidential data could be intercepted. The only exception to this is Councillor email addresses.

The Council does not use an e-mail archiving system and therefore recommends that users keep any critical emails in their departmental folder.

Relevant Legislation

Under Section 77 of the Freedom of Information Act 2000 and Regulation 19 of the Environmental Information Regulations 2004 it is an offence to destroy information where there is a current FOI or EIR request being dealt with. Section 8 (6) of the Data Protection Act 1998 states that the data to be supplied to an individual requesting it must be the data that was available at the time the request was received. Under Section 13 of the Data Protection Act (DPA), individuals can claim compensation where they have suffered damage resulting from the Council's non-compliance with the DPA.

It is therefore essential to ensure that no e-mails are deleted that are needed in connection with any of these requests or in connection with any litigation cases that may arise. Once information is destroyed in accordance with the Council's Records Retention and Disposal Policy, the Council is then under no obligation to provide that information in response to requests for information. It is only an offence to delete the information where there is a current request.

Further, under the DPA the Council should not retain personal information about individuals for any longer than is needed, therefore the deletion of personal information where retention is no longer necessary will comply with the DPA.

And finally…
Before starting the e-mail, think if it is the most suitable medium for the message. If the email deals with sensitive, complex or confidential matters it may be more appropriate to use the phone or speak to someone in person.

Access Control

Responsibilities

All staff shall ensure that:

- They gain access to systems through official means;
- They take responsibility for all use of their network password, or any others assigned to them;
- They do not share their password, or allow anyone to use it unsupervised; and
- They report immediately any misuse of their account.

Line and Service Managers shall ensure that:

- They make requests for access as early as possible, using an Access Request Form for new starters, and request changes via email;
- They only request the minimum access to allow the staff to perform the tasks appropriate to their role and responsibilities;

- They keep track of the access that staff have and be mindful to remove all access from staff that has changed department or role. This is especially important during reorganisations;
- ICT is informed as soon as possible when a staff member is leaving; and
- Where a staff member is under investigation or has left under difficult circumstances thought is given to restricting their access. Remember that some systems may be available from home, not just in the office.

System Owners shall ensure that:

- Security controls on their system are robust and only grant to minimum access required for any particular role;
- Administration level logins are not routinely used and are protected;
- Requests for system access that are not appropriate are denied;
- Where they suspect a login is being abused they inform ICT;
- They annually review all logins to their system;
- Where they suspect a login is no longer required they contact the appropriate manager; and
- They inform ICT of any access or security changes.

ICT shall ensure that:

- Each user shall be assigned a unique user ID, which is not reused;
- Appropriate security controls are in place to protect the Council's data;
- Network accounts are protected from misuse;
- Access to data and systems are properly authorised;
- They co-ordinate with system owners;
- They co-ordinate with Personnel to remove access from leavers that Managers have failed to report; and
- They monitor and remove unused network accounts.

User-registration Procedure

In order to setup a new network account, ICT must receive a completed 'IT Services Access Form' (available via the intranet) for the new user, authorised by the Line Manager or Service Manager. All access requests made for Agency staff must stipulate a termination date.

ICT will confirm with Personnel that the new user request is actually for a genuine new member of staff. Agency staff will be verified by the requesting manager's, line manager.

The network account will be created, but login credentials will remain undisclosed to the user until a signed copy of the Personal Data Security Commitment is received.

Any system access on the form will be passed to the appropriate system owner to authorise and set up.

Login credentials and training forms will passed to the departmental IT coach in a sealed envelope, addressed to the new user and marked “Confidential”. They will then provide the basic training. The system will require the password to be changed on during the first logon.

The level of access granted will be appropriate for the intended business purpose and the employee’s roles and responsibilities.

De-registration Procedure

When an employee leaves the Council, access rights should be withdrawn immediately. Line Management will liaise with ICT and decide whether the account’s incoming e-mail is to be deleted immediately or monitored for a period of time before deletion.

It is the responsibility of all Line Managers and Service Managers to inform ICT of all staff leavers, via the ‘IT Services Access Form’ (available via the intranet) or via email.

All access requests made for Agency staff must stipulate a termination date. Where this is not stated, the account will be automatically disabled after 1 month. The line manager will need to contact ICT in order to re-enable the account if access is still required.

Personnel will provide ICT with monthly Starters, Leavers and Amendments list, which is utilised to ensure all Council staff leavers are promptly disabled on the network.

ICT will pass leaver information to system owners to ensure system access is also removed.

Amendment Procedure

When an employee moves from one section to another, it is the responsibility of the previous Line/Service Manager to complete the ‘IT Services Access Form’ for the revocation of privileges, and the new Line/Service Manager to complete another ‘IT Services Access Form’ for the registration of new access. As the user already has a form, it is also acceptable to take the changes via email from the old and new managers. This information is then added to the user’s access form in the filing system.

Any system access changes will be passed to the appropriate system owner to authorise and set up.

Training

Departmental IT Coaches will provide initial training to staff members when they first get their network account. This will cover:

- Signing off of the Personal Data Security Commitment and provision of information about this policy;
- Finding more information, particularly on the Intranet;
- Advice and pointers on the health and safety aspect of display screen equipment (DSE);
- Correct use of the network account and the computer's basic security features;
- The correct locations to store data to ensure it is protected correctly; and
- Guidance on the acceptable use of equipment;

The user will sign to confirm they have received this training.

Further to this, users of computers will have mandatory Data Protection Training provided by Legal Services.

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and a poorly chosen password could result in the compromise of the Council's network and applications. As such, all users with access to the Council's systems are responsible for taking the appropriate steps as outlined below, to select and secure their passwords.

Password Use

Terminals must not be left unattended when 'signed on'. If not in constant use, 'sign off' or lock the computer. Computers will lock automatically if not in use. Do not leave computers locked for a long time, log off or shut down instead.

It is acceptable to log on to a PC and have another person use it, for example for training, demo or presentation purposes; however users must supervise this person at all times and the user is responsible for anything the temporary user does on the account.

Where passwords are used to encrypt documents, do not send the password via the same method as the encrypted file. For instance if the file is emailed, telephone the password through or send a fax, do not send it by email, even if it is a separate email sent later. If the file is sent on CD or USB the password could be emailed. If you do not protect the password, the file may as well not be encrypted.

Password Policy

The following guidelines give information on how passwords should be created and managed to ensure their integrity and the integrity of the systems and information which they protect.

The following best practice guidelines should be followed at all times, though it is recognised that some systems may be unable to support some of the recommended guidelines, due to technical limitations.

Password Requirements

To ensure that malicious parties or programs which guess passwords have a reduced chance of being successful, users should construct a password that meets the minimum criteria for each system as shown in the table below.

System / Type	Minimum requirements	Lockout / Wipe
Network Accounts and Council Computer Systems	8 characters, 3 out of 4 of upper, lower, numbers and symbols	Locks out after 10 attempts
Smartphones and tablets	4 characters, at least one of each letter, number and symbol	Wipes device after 10 attempts
Administration passwords	10 characters, 3 out of 4 of upper, lower, numbers and symbols	Lock out after 10 attempts
Files protected with strong encryption systems (such as WinZip AES-256)	15 characters, use all of upper, lower, number and symbols.	Unlimited attempts, file has no protection
Note these are minimum lengths, longer passwords will be a lot stronger For other systems ICT will investigate and decide an appropriate password scheme		

To make sure the password is strong users should also ensure that passwords:

- must not contain the user login name;

- must not include the user's own or relative's name, employee number, national insurance number, birth date, telephone number, car licence plate or any information about him or her that could be readily learned or guessed;

- should not be single words from an English dictionary or a dictionary of another language, slang, dialect or jargon with which the user has familiarity. This is true even with a number placed at the end;

- are significantly different from previous passwords and password used for other systems. Do not reuse old passwords or words spelt backwards;

- do not contain commonly used proper names, including the name of any fictional character or place;

- do not contain any simple pattern of letters or numbers such as “12345678” or “abc123”, or deliberately misspelled words;

- are not displayed in work areas or any other visible place. If a user has to write their password down, they must ensure it is kept as securely as, for example, their credit card. Write down only the password, not the system it is for and if possible include a mistake. Inform ICT should this go missing;

- are not e-mailed, recorded electronically, or used via the “save password” functionality which may result in a password being taken or shared;

- Finally, be careful when using systems which allow users to enter a password reminder or hint; the reminder or hint must not be the user's name, password or text which clearly identifies the password (e.g. child's name) as this is a security risk, and users MUST NOT let anyone observe them when entering their password.

Password Changes / Life Expectancy

Network passwords must be changed in line with the following rules:

- At least every 90 days for all users;

- On receiving a new or reset password;

- As soon as possible after a password has been compromised or after a suspected compromise;

- On direction from the Council’s ICT staff;

- Passwords are deactivated on leaving the Council; and

- Administrator passwords should be changed whenever a member of staff leaves the Council who had administrator access.

Password Suspension

The network will permit ten attempts to enter the correct User ID and password before the account is locked. It will unlock after 30 minutes so can be tried again. Smartphones and tablets allow ten attempts before wiping the device.

When an account has been suspended, it can be released by the appropriate system administrator. In the case of the network (log on) or systems managed by ICT requests for release of suspended accounts should be made via the ICT Helpdesk.

To reset a password for individual applications, the relevant System Owner for that system should be contacted.

Password and Account Protection

NOTE: Each user is responsible for all activities originating from any of his or her username(s).

Passwords must **NOT** be shared. Users who share their passwords may have their access to the Council’s networks and systems disabled, whilst investigations are carried out and management determine the course of action (disciplinary) that may be required.

Password Construction

Creating strong passwords does not have to be difficult, try this method.

What to do	**Example**
Start with a sentence or two	Longer passwords are safer.
Remove the spaces between the words	Longerpasswordsaresafer.
Add shorthand and misspell words	LingerpasswordsRsafer.
Add length with numbers and symbols, don't always do this at the start or end.	LingerpasswordsRsafer1999.

While this password is fairly easy to remember the number of combinations an attacker would have to check is huge. Even if an attacker can check billions of passwords a second on thousands of computers it would still take too long to find the password.

You can use the Microsoft password checker to check the strength of a password similar to the one you are planning to use. This is particularly important for files where the number of attempts that can be made is unlimited.

https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

Use only this password checker, and only to get a feel for password security, do not input any real passwords.

Remote and Mobile Access

For all remote and mobile access adhere to the Off Site Security guidelines.

Remote Access

Authorised users and external organisations may be granted remote access to the network based upon job requirements and business criteria deemed appropriate by the Council and/or System Owners.

Note: ***Remote access shall not be used to connect to or use any Public Services Network applications or data***.

‘Full’ Network and Application Remote Access

The following guidelines will be adhered to by all remote staff users:

- In order to gain remote access please refer to the Occasional & Permanent Home Working Policy;
- Remote Access will be carried out through the corporate remote access systems requiring an Access Token;
- Only authorised personnel will be provided an Access Token and associated credentials. Tokens must be stored securely when not in use. Loss of an Access Token should be reported immediately to ICT ext 3888 to allow the access to be disabled;
- Never share Access Tokens, PINs, passwords or any other access mechanisms; and
- All remote computers accessing the network must use Council machines, and the Council’s certified anti-virus, firewall and other security software.

Use of Laptops

Certain post holders will be provided with laptops due to the nature of their work. Laptops are also available as loans for ad hoc requirements.

The following guidelines apply to the use of Council laptops:

- All laptops shall have full disk encryption;
- Laptops must be connected to the network at least once per week to download security updates, including anti-virus. Please ensure the PC is given sufficient time on the network to download the updates, do not defer their installation;
- Although the laptop is encrypted, authorisation from the user’s Manager must be obtained prior to taking Council data off site.

Web Mail Access

Web Mail is currently used by Councillors to access their email, and by other users on an ad hoc basis. Two factor authentication must be used to prevent unauthorised access should the password be stolen.

Access is allowed from personal computers, however they must meet the following minimum security standard:

- The operating system in use is fully supported and has all available security patches loaded. Security patches should be set up to load automatically;
- All software on the PC should also have security patches loaded;
- Antivirus/Antimalware software should be installed and up to date;
- A firewall should be in place which restricts access to the device;
- The web browser on the PC should be fully patched and relevant security features enabled.

When using Web Mail:

- Do not use it on public or shared PCs, for example hotel, café or library PCs, only use it on trusted PCs;
- Make sure it is not overlooked;
- Do not allow the computer to store the password;
- Make sure log off correctly completed.

Remote Access for Supplier Support

Remote access by external organisations will adhere to the following guidelines:

- A request should be made to the System Owner and ICT informed;
- Access will only generally be in office hours so the dial in may be monitored and logged by ICT;
- Access will only be granted via ICT approved methods;
- When the organisation has finished accessing the Council's resources remotely for a particular task, they must promptly disconnect from the network.

Please refer to the Remote Working policy and ICT for further advice.

Mobile Devices

Note: ***Mobile access shall not be used to connect to or use any Public Services Network applications or data***.

Responsibilities

All mobile device users shall ensure that:

- They only utilise mobile devices which have been acquired, configured and issued by ICT Services;
- They take reasonable care of any issued mobile device;
- They safeguard personal data, including passwords and any other access codes;
- They comply with the Data Protection Policy. If in doubt; details of identifiable individuals must not be stored on any mobile device;
- They report all lost/damaged mobile devices to the ICT Helpdesk, on ext 3888;
- They **DO NOT** disable or deliberately seek to circumvent the security controls applied by ICT Services;
- They **DO NOT** try to access unapproved 'networks' when using Council issued mobile devices;
- They **DO NOT** use Council mobile devices to produce, obtain, store, display or distribute material that is likely to cause offence to others or is illegal

- They **DO NOT** copy or in any way distribute any software which is integral to Council mobile devices;
- They accept that mobile devices can be used for personal use the cost of which is to be reimbursed using establish procedures (primarily mobile calls and text usage);
- Contact details are stored on the SIM and not directly onto the phone with the exception of smartphones and tablets where contact details should be stored within the Council's corporate office management system (currently Microsoft Outlook);
- For devices with no centrally enforced password, the power on pin control facilities are enabled;
- They accept that SIM cards must not be removed or transferred to any other mobile device;
- They request and obtain authorisation from ICT Services prior to re-allocating any issued mobile device to another authorised user;
- The transfer of 'information' to and from the Council's network using 'authorised facilities' only takes place with the approval of the Information Asset Owner and, due regard is given to the requirement for encryption depending on the Information Asset Class;
- With the exception of devices which are capable of encrypting images, digital cameras are not be used to capture sensitive or personal information;
- Digital Cameras are used in accordance with the Council's photographic policy;
- Users who deploy the Bluetooth functionality ensure that all 'contact' details are removed from any 'paired' device prior to the disposal of or transfer of ownership (for example; where contacts have been 'copied' into a Car's Bluetooth System);
- Paper records containing confidential or sensitive information are kept secure and totally separate from valuable items such as laptops; and
- They never establish connections to the Council's network from outside the UK. The only exception is the Chief Executive Officer who is allowed to use their Mobile Device abroad to allow them to respond to Council emergencies.

ICT Services shall ensure that appropriate security controls are in place and measures undertaken to protect the Council's Information Assets.

Mobile Device Deployment Arrangements

SIM Connectivity

SIM only connectivity is usually deployed in association with 'application specific' solutions the arrangements for which are dealt with within the remote working policy. Examples include:

- Car park pay stations, and/or
- Hand held or vehicle cab mounted devices.

Mobile Phones

The Council deploys the following 'standard' mobile phones:

- A basic device which is capable of making, and receiving voice calls and texts, has voice mail and a 'contacts' facility; and
- A device which has all the basic features and has an integral camera which is suitable for the capture of images which do not include personal information.

These devices are not connected to the Council's Network.

Smartphones & Tablets

A device which is capable of making, and receiving voice calls and texts, has voice mail (not tablets), contacts, a camera and access to the Internet. These devices are not connected to the Council's Network directly but may have access such as mail, calendar and other services.

Feature Restrictions

The following features have been disabled for all mobile and smartphones:

- Premium rate services; and
- International dialling.

Mobile device deployment arrangements

Device	Issue Criteria
SIM Only	Usually deployed in associated with a ‘specific application’ see remote working policy
Basic device	Office based visiting Officers, On Call Officers, external lone workers, Field Officers, Officers who attend regular off site meetings who need stay in contact with base and Councillors
Camera enabled device	Office based visiting Officers with a requirement to take reasonable quality images where encryption is not required for example, buildings, land and trees etc.
Smartphone or tablet	On Call Officers, where the duty is shared and access to the Internet is essential Officers who spend a considerable amount of time out of the office and/or need the additional functionality provided by these devices. In instances where images are being taken of personal information for example prime documents in support of Housing Benefits Councillors

The issue of mobile devices must be approved by Service Managers. The issue of mobile devices to Councillors must be approved by the Corporate Director responsible for Member Services.

Mass Storage Facilities (removable media)

Any transportation of ‘data’ must be undertaken with due regard to its ‘classification’. The Data Management section provides more information on this subject but in summary, extreme care must be taken when removing ‘restricted’ or ‘protected’ data for any reason.

Prior to using any removable media option, consideration must have been given to other ‘transportation’ options including the use of the Public Services Network and other ‘secure’ Network Connections.

Where other, ‘appropriate’ data transport options have been considered then mass storage (removable media) options can be utilised. Mass storage facilities include any portable device which is capable of being ‘connected’ to the Council’s network via a desktop workstation onto which data can be transferred. Mass Storage facilities include:

- USB Data Pens;
- CDs;
- DVDs;
- Digital Cameras; and
- External Disk Drives.

The Council has arrangements in place to manage the utilisation of digital cameras. This includes dedicated cameras and cameras which are an integral part of a multifunctional device.

Data can only be transferred on Council approved devices and all sensitive data must be protected with strong encryption. Such approved removable media devices are only to be used for the purpose requested and authorised. Their connection to any other systems for which their use was not explicitly authorised remains prohibited.

Only authorised devices will be allowed to connect to the Council's network. This will be managed through device control software and systems deployed by ICT.

Breach Guidance

The following are examples of policy breach all of which must be appropriately reported:

- Loss of a mobile device and/or associated accessory;
- Damage of mobile device and/or associated accessory;
- Unauthorised configuration activity;
- Inappropriate use of a mobile device;
- Unauthorised re-assignment of a mobile device; and
- Unauthorised SIM card activity.

All instances of policy breach must be reported to ICT at the first opportunity via the ICT Helpdesk on ext 3888.

Network Access Control

All boundaries between different networks shall be controlled by firewalls. This includes Public Services Network, the DMZ, other WAN connections to other Councils and the Internet. These firewalls shall be configured with the minimum access required to achieve the business objective. Requests for overly permissive rules may be denied to protect the rest of the network. Changes must be approved by the ICT Technical Manager. Other network controls and routing shall be used where appropriate to increase the security of information.

Wireless Networking

Wireless networks such as WIFI can be very useful for mobile devices but their uncontrolled use can provide a means for attackers to access the network from beyond the physical security barrier. We must therefore minimise this risk.

All Staff shall ensure that:

- They only connect Council Laptops and Tablets to wireless networks that they trust, avoid using unknown or public hotspots where possible;
- On the Council's network they only use wireless networking systems provided by ICT;
- Follow any instructions given in the use of the Council's wireless networks;
- Do NOT connect any wireless networking equipment to a PC or the network;
- Do NOT configure Device Tethering, Access Point sharing or similar technologies on Council equipment without authorisation from ICT;
- They alert ICT if they suspect unauthorised wireless equipment is being used.

ICT Services shall ensure that:

- Wireless networks are configured using a secure best practise configuration;
- Wireless networks are independently assessed for security weaknesses each year;
- Wireless networks in use by the Public or non-Gedling staff are appropriately segmented from the main network, ideally physically separate;
- Quarterly scans are conducted to identify unauthorised wireless access points;
- Unauthorised wireless access points are immediately removed from the network;
- Report unauthorised wireless access to the Data Security Group.

Information Security Incident Management

The Data Security Breach Management Policy seeks to outline the measures to be taken by the Council when dealing with a data security breach. It applies to information in all forms, whether manual or computerised. The aim of this policy is to ensure that the Council reacts appropriately to any actual or suspected security incidents relating to information systems and data. Appropriate action following a breach is required to ensure containment and recovery, business continuity and to avoid further breaches of the law and statutory, regulatory or contractual obligations.

Data Security Breaches

A data security breach can happen for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored including paper files;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Inappropriate disposal of information;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it. (This is also referred to as "social engineering");
- The transfer of data or information to those who are not entitled to receive that information;
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system; and
- The unauthorised use of an authorised system.

Further examples of data breaches are provided under Examples of Data Security Incidents.
Any breach, however it occurs, can have far reaching consequences. It could cause potential harm and distress to individuals or seriously compromise the integrity and security of the Council's IT systems. As a result, this Policy seeks to recognise the following four important elements:

- Containment and recovery;
- Assessment of ongoing risk;
- Notification of breach; and
- Evaluation and response.

Responsibilities

<u>Overview</u>

It may transpire that assistance is required from ether IT Services, Legal Services or Audit and Risk Management to 'determine' the nature of the 'incident' the details of which would pass to the Service Manager for determination.

Therefore, the Data Security Group in this context is assisting the Council to remain ‘compliant’ and ‘helping’ to resolve ‘incidents’ in a sensible and pragmatic fashion.

All staff shall ensure that:

- All breaches of information security and the Data Protection Act, actual or suspected, are reported to a line manager or Service Manager as soon as possible;
- All breaches of information security and the Data Protection Act, actual or suspected, which occur or are discovered outside of normal office hours are reported to a line manager or Service Manager immediately the next working day. A voicemail message may be left out of hours, but will not be sufficient on its own. It must be followed up the following working day as soon as the Council offices are open to ensure that the report has been received and it being dealt with;
- They co-operate fully with any investigation following a data security breach; and
- They report any instances where the Policy has been or is being violated to the ICT Helpdesk, ext 3888.

All Line Managers and Service Managers shall ensure that:

- All breaches of information security and the Data Protection Act, actual or suspected, are reported to a member of the Data Security Group as soon as possible; and
- They co-operate fully with any investigation following a data security breach.

A Member of the Data Security Group will:

- If invited, decide who will take the lead on investigating the breach and ensure the investigation is completed in a timely fashion;
- Establish who needs to be made aware of the breach and inform them what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door;
- Establish whether there is anything the Council can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts;
- Assess the risks associated with the breach, which requires consideration of how serious or substantial they are and how likely they are to happen. This includes risks to the Council's IT systems and potential adverse consequences for individuals;
- Consider what steps need to be taken to prevent further breaches;
- Consider what other agencies may need to be informed depending on the type and severity of the breach.
- Consider whether Warning, Advice and Reporting Point (EMG Warp) should be consulted; and
- Report the outcome of the investigation to the Service Manager

The Service Manager shall:

- Consider the information gathered as part of the investigation and implement the steps which need to be taken to:
    - contain the breach and recover any losses; and
    - reduce or remove any ongoing risks; and
    - prevent any further breaches.

Notification of Breaches

The Monitoring Officer in conjunction with the Chief Financial Officer and relevant Corporate Director will decide whether it is appropriate to notify:

- The individual(s) affected by the breach;
- The Information Commissioner;
- Public Services Network team (where incidents impact the PSN);
- The Press; and/or
- CESG GovCertUK;

The Chief Executive will ultimately determine whether it is appropriate to notify the press,

The Council recognises that informing individuals and organisations it has experienced a data security breach can be an important part of security breach management, however, notification should have a clear purpose.

Notifying Individuals

The Council recognises that not every incident will warrant notification and notifying everyone whose details are held on a database of an issue affecting only a small proportion of those people may well cause disproportionate enquiries and work.

Individuals affected will be notified if necessary to enable them to take steps to protect themselves, for example by cancelling a credit card or changing a password, or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. When notifying individuals, the Council will endeavour to give them specific and clear advice on the steps they can take to protect themselves and also what the Council is able to do to help them.

Notifying the Information Commissioner

There is no legal obligation on the Council, as a data controller, to report breaches of security which result in loss, release or corruption of personal data, to the Information Commissioner. However the Council considers it is appropriate to bring serious breaches, where a large number of people are affected, or there are very serious consequences, to his attention.

The following will be considered when deciding whether a breach should be reported to the ICO:

- The potential harm to data subjects. This could be exposure to identity theft through the release of non-public identifiers e.g. passport number or information about the private aspects of a person's life becoming known to others e.g. financial circumstances. The extent of harm, which can include distress, is dependant on both the volume of personal data involved and the sensitivity of the data. Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there will be a presumption to report.

Where there is little risk that individuals would suffer significant harm, the breach will not be reported.

- The volume of personal data lost / released / corrupted.
  There is a presumption that the Council will report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Every case must be considered on its own merits but the Council would expect to report a security breach concerning information relating to about 1000 or more individuals.

  However, it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high, perhaps because of the circumstances of the loss or the extent of information about each individual.

- The sensitivity of the data lost / released / unlawfully corrupted.
  There is a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA. As few as 10 records could be the trigger if the information is particularly sensitive.

Notifying the Press

When considering whether to inform the media, the Council will balance the need to be open and transparent with the need to protect the interests of those individuals who may suffer distress at having the breach reported in the press, together with the risks of unscrupulous individuals who may seek to take advantage of the situation. Advice will be sought from the Council's Communications Team prior to any decision being made as to what, if anything is reported.

The Chief Executive will ultimately determine whether it is appropriate to notify the press.

Notifying CESG GovCertUK /
GovCertUK is responsible for providing support to local authorities when responding to computer security incidents. As a member of Public Services Network, the Council is required to report critical and significant security incidents to GovCertUK.

The CESG categorises incidents (depending on their scope, number of users affected, ability of the Council to deal with the situation and impact), into Negligible, Minor, Significant and Critical categories. Some examples are:

Negligible: Spam, Quarantined viruses, network monitoring alerts on single PCs.
Minor: Unsuccessful denial of service on a single PC, single PC unauthorised access.
Significant: Successful denial of service on a server, website defacement.
Critical: Targeted attack on our network infrastructure, unauthorised access to a server.

Generally Significant and Critical incidents have to be reported, minor can be reported for information collation purposes while negligible incidents do not have to be reported. The document also discusses which agencies should be informed about different types of incidents.

The Chief Financial Officer in conjunction with the Monitoring Officer will make the decision. In doing so, they will take into account the CESG GovCertUK Incident Response Guidelines which apply at that time.

Public Services Network (PSN) / CINRAS

For incidents that impact on Public Services Network, the “Incident and Problem Management” process manual should be consulted and if appropriate the incident reported to the PSN Security Manager. The decision to do so will be made by The Chief Financial Officer in conjunction with the Monitoring Officer.

CINRAS shall be notified for incidents involving HMG approved cryptographic equipment.

Notifying other agencies/organisations

The Council will consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

Emergency Situations

The Council recognises that that there may be instances where immediate action is necessary to contain a breach and prevent further incident. An example is where there is a targeted attack resulting in a serious breach of network security. This would require immediate action to shut down the Council’s network. It would not be practical or reasonable for a full investigation to be carried out as outlined in this Policy. Instead, the Customer Services & IT Manager and IT Technical Manager have the authority to take whatever action they deem necessary in the circumstances and would follow the procedure outlined above to determine what further action should be taken.

Examples of Data Security Incidents

Examples of some of the most common Data Security Incidents are:

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically;
- Computer infected by a Virus or other malware;
- Sending a sensitive e-mail to 'all staff';
- Finding data that has been changed or accessed by an unauthorised person; and
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on the Council’s equipment;
- Use of unapproved or unauthorised hardware on the Council’s network/equipment;
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password);
- Writing down a password and leaving it on display / somewhere easy to find;
- Printing or copying confidential information and not storing it correctly or confidentially;
- Responding to or forwarding unsolicited mail of an offensive nature; and
- Responding to or following links in unsolicited mail which require entry of personal data.

Theft / Loss

- Theft / loss of a hard copy file;
- Theft / loss of any of the Council’s computer equipment; and
- Theft / loss of removable media [USB / memory sticks].

Data Management

The Council's partnership working with Central Government and other national bodies and agencies has led to the exchange and sharing of information that requires protection and handling in line with the requirements of the Public Services Network and the Government Security Classifications Policy (GSCP). The GSCP describes how HM Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

Organisations which work with government have a duty to respect the confidentiality and integrity of any HMG information and data that they access, and are accountable for safeguarding assets in line with the GSCP.

Purpose and principles

The purpose of this Data Management Policy is to ensure the Council meets its obligations under the GSCP and also has appropriate controls in place to protect its own information. It reflects the following principles:

Principle One: All information that the Council collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

Principle Two: Everyone who works with the Council (including staff, members, contractors and partners) has a duty of confidentiality and a responsibility to safeguard any Council information or data that they access, irrespective of whether it is marked or not, and is must be provided with appropriate training.

Principle Three: Access to sensitive information must be granted on the basis of a genuine "need to know" and subject to an appropriate personnel security control.

Principle Four: Assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

Classification / Categorisation of the Council's Information Assets

The GSCP classifies HMG information assets into three types: OFFICIAL, SECRET and TOP SECRET.

The Council operates exclusively at OFFICIAL level and the previous classifications, RESTRICTED, PROTECTED and UNCLASSIFIED no longer apply.

The main theme of the new Government policy is, at OFFICIAL at least, personal responsibility for the data you transmit, handle or store, no longer relying on security markings. This is particularly important because the UNCLASSIFED marking no longer exists.

OFFICIAL information

The OFFICIAL level covers the variety of information handled and created by the Council of differing value and sensitivity and different consequences resulting from loss of compromise.

Some of the Council's information is particularly sensitive and could have more damaging consequences (for individuals, the Council or partner) if it were lost, stolen or published in the media This sensitive information will attract additional controls to ensure that it is only accessed by those with a "need to know". Such information should be treated as OFFICIAL–SENSITIVE.

Guidance on what information should be treated as OFFICIAL–SENSITIVE and how it should be handled appears below.

It is important to note that within the GSCP CONFIDENTIAL is not a recognised security classification; therefore care must be taken if marking documents as confidential. It must be clear to the recipient of the information what this means and what handling requirements are to be applied.

Marking OFFICIAL information

There is no requirement to explicitly mark routine OFFICIAL information.

Security markings previously applied to council information which now fall in the OFFICIAL classification can therefore be removed.

Handling OFFICIAL information

All Council information must be:

- Handled with care to avoid loss, damage or inappropriate access.
- Shared responsibly, for business purposes, and using appropriately assured channels if required (e.g. GCSX secure email).
- Stored securely when not in use. For example, with clear desk policies and screens locking when ICT is left unattended.
- Protected in transit and not left unattended when taken out of the office.
- Stored securely when taken out of the office. For example in a locked briefcase or locked cabinet.
- Protected to prevent overlooking or inadvertent access when working remotely or in public places.
- Discussed with appropriate discretion when in public or over the telephone. Details of sensitive material should be kept to a minimum.

- Emailed, faxed and sent by letter only to named recipients at known addresses.
- Destroyed in a way that makes access unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

The following table sets out the minimum controls that should be applied:

	OFFICIAL
Principles and clearance levels	Appropriate training delivered which reinforces personal responsibility and duty of care
Document handling	Clear desk / screen policy
Storage	Storage under single barrier and / or lock and key Laptops must be kept secure at all times and locked away overnight when left in the office
Remote Working	Permitted with line manager approval Ensure information cannot be inadvertently overlooked whilst being accessed remotely Papers/laptop must be stored out of sight Papers/laptop must not be left in a vehicle overnight
Moving assets by hand	Single cover Ensure information cannot be inadvertently overlooked when working in transit Approval of senior manager must be obtained to move a significant volume of records (100s) /files (10s) from the office Approval must be subject to an appropriate assessment of risk and appropriate controls applied
Moving assets by post / courier	Single cover
Electronic Information at rest	Electronic Information needs to be saved on the network where it will be protected at rest in a physically secure data centre with access control groups applied Laptops must be encrypted Alternative storage (e.g. G Cloud/hosted website) can only be used if approved by ICT
Electronic Information in Transit	Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption May be emailed / shared unprotected to external partners / citizens, however consideration must be given as to whether that is an appropriate method of transmission. This must be determined on a case by case basis and where additional protection is considered necessary, the information must be encrypted or password protected (*See below for specific guidance on transmitting personal data) Approval of senior manager must be obtained to email a significant volume of records (100s) /files (10s). Approval

	must be subject to an appropriate assessment of risk and appropriate controls applied
Removable Media (data bearing)	The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement Consider appropriate encryption to protect the content, particularly where it is outside the Council's physical control
Telephony (mobile and landline), Video Conference and Fax	Can be discussed over the telephone with appropriate discretion Faxes must only be sent to named recipients at a known fax number
Disposal of paper documents	Must be disposed of with case making reconstitution unlikely Tear document into small pieces and place in recycling bin
Disposal of digital equipment and media	See Secure Disposal or Re-use of Equipment

Special Instructions when handling personal data

The seventh principle of the Data Protection Act states that:

> "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Whilst personal data will generally fall in the OFFICIAL classification, additional controls must be observed to ensure that the Council complies with its obligations under the Data Protection Act.

- Original certificates (e.g. birth certificates, medical records, passports) should be transferred / returned by Tracked Courier;
- Multiple and restricted lists (e.g. names and addresses) should be sent by Tracked Courier and if held on electronic media, strong encryption should be used with a strong password (see Password Policy);
- Paper records containing personal data must be kept secure when off-site in a lockable case and totally separate from valuable items such as laptops;

- Access to Public Registers (e.g. Electoral Register) should be supervised for viewing only, copies must not be provided or downloaded unless under statutory authority;
- 3rd party suppliers (e.g. printing of Council Tax bills) where electronic files of data are transmitted should be sent by secure FTP on a link already set up;
- Partnership arrangements where electronic files of personal data are transferred should be by secure electronic methods only and encrypted except for Public Services Network. (GCSx email is inherently secure and does not routinely need encryption);
- An individual's personal data may be sent by unencrypted email where they have given the Council permission to send via unsecured email. The individual must also acknowledge that we cannot be held responsible if a 3rd party gains the information after the Council has sent it;
- It is the user's responsibility to ensure that the recipient's email address is correct and the receiver is ready to handle the information being sent in the required format. Specific care must be taken to ensure that personal data is not sent to recipients on a contacts list;
- Fax machines must only be used to transfer personal data where it is absolutely necessary to do so. The following rules must apply:
    - The sender must confirm with the intended recipient that the fax machine is located in a secure location where only staff who have a legitimate right to view the information can access it or that the intended recipient is waiting by the fax machine to receive the transmission;
    - The sender is certain that the correct person will receive it and that the fax number is correct;
    - The sender notifies the recipient when sending the fax and asks them to acknowledge receipt;
    - Care is taken to ensure the correct number is dialled. When a fax number is entered manually the sender must check the recipient's fax number against the fax cover sheet;
    - The sender must ensure that the fax confirmation sheet is checked as soon as possible after transmission to confirm that the receiving fax number and number of sheets transmitted are correct;
    - Confidential faxes must not be left lying around for unauthorised staff to see;
    - Only the minimum amount of personal data should be sent, and where possible the data should be anonymised or a unique identifier used;
    - Faxes sent should include a front sheet which contains a suitable confidentiality clause;
    - Pre-programmed fax numbers must be checked regularly to ensure that they are still valid;
    - If anything appears wrong when transmitting a fax, the call must be suspended immediately and the sender's Service Manager notified of a possible data breach.

- When printing personal data, staff must check that all print jobs that start are completed. Where jobs cannot complete (e.g. owing to a printer error) staff must ensure that they are deleted from the print queue. Failure to do this could result in the print job resuming in their absence, and result in personal data being left out on the printer;
- When printing personal data, the document must be removed from the printer immediately. Personal data must never be printed to a printer accessible to the public unless the secure print facility is used;
- All unwanted printed material containing personal data must be shredded using the cross cut shredder facilities provided.

OFFICIAL-SENSITIVE information

OFFICIAL-SENSITIVE is not a separate classification; it is simply a tool to identify OFFICIAL information that is particularly sensitivity and needs additional controls.

OFFICIAL-SENSITIVE should be used by exception and in limited circumstances where there is a clear and justifiable reason to reinforce the "need to know." This would be when compromise or loss of the information could have particularly damaging consequences for an individual (or group of individuals), a partner, or the Council.

Some examples of OFFICIAL-SENSITIVE information are as follows:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to members on contentious and very sensitive issues;
- commercial information e.g. contract negotiations that may be damage/undermine the Council or commercial partner's negotiating position if improperly accessed;
- information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- sensitive personal data;
- legal advice and information created in connection with legal proceedings.

Determining whether information is OFFICIAL-SENSITIVE

The originator of the information is responsible for determining the appropriate classification for any assets they create, with reference to this Policy, and marking the asset where OFFICIAL-SENSITIVE.

The originator must understand the business value and sensitivity of the information they create. Information should not be regarded as OFFICIAL-SENSITIVE as a matter of routine as applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls. However, not applying the OFFICIAL-SENSITIVE marking to sensitive assets may result in inappropriate controls and potentially put them at greater risk of compromise.

Responsibility for any change in the classification lies with the originator. Recipients must not re-classify a document without the agreement of the originator. Where that agreement cannot be obtained, for example because the originator no longer works for the Council, agreement must be obtained from the originator's manager.

Marking OFFICIAL-SENSITIVE information

OFFICIAL–SENSITIVE information must be clearly marked to indicate the need for further controls. Failure to apply the appropriate protective marking could result in the compromise of sensitive information handled and created by the Council.

All electronically produced documents that require protective marking shall be page numbered and have the protective marking in capitals on each page to ensure the protection of the information within the document as follows:

Page # of #
Protective Marking: OFFICIAL-SENSITIVE

Emails which carry a protective marking of OFFICIAL-SENSITIVE must be clearly marked in capitals as such in the subject line of the email.

All other documents that require protective marking shall be marked by handwriting with permanent ink in capitals on each page of the document OFFICIAL-SENSITIVE.

The originator of the document should exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate. For example, by writing conspicuously within the email or on the front of the document:

- “This information has been produced by GBC. Please do not distribute this document further without the approval of the sender”.
- “contains legal advice and should not be copied or shared outside the Council”.

- “contains sensitive personal information. This is for your eyes only – it remains highly contentious and should not be copied any further.”

Handling OFFICIAL-SENSITIVE information

The handling requirements for OFFICIAL information set out above must be adhered, but the following table sets out additional controls should be applied:

	OFFICIAL-SENSITIVE
Principles and clearance levels	Access limited to those with a “need to know‟
Document handling	Not to be left unattended and must be locked away when not in use
Storage	Storage in a locked cabinet or controlled storage area

Remote Working	Stored under lock and key in briefcase or cabinet Limit the amount of information taken out of the office to what is strictly necessary Information must not be emailed to personal/home email accounts in order to work remotely Papers/laptop must not be left unattended
Moving assets by hand	Must be accompanied at all times Envelope/package is closed and the word OFFICIAL-SENSITIVE is not visible
Moving assets by post / courier	Outer envelope must be addressed to a named individual Outer envelope must include return address in case delivery is unsuccessful Outer envelope must not include or show the marking OFFICIAL-SENSITIVE Double envelope and mark the internal envelope OFFICIAL-SENSITIVE Consider using registered Royal Mail service or reputable commercial couriers "track and trace‟ service
Electronic Information at rest	Must only be saved on the network or approved encrypted council device Must be saved with OFFICIAL SENSITIVE in the title Password protection must be applied to individual document Password must only be shared with those with a "need to know"
Electronic Information in Transit	Must only be sent to known contacts with a "need to know" Must be encrypted or sent via secure email such as Public Services Network (GCSx) email Must not be transmitted to private email accounts (including employee/member personal email accounts) or generally across the internet
Removable Media (data bearing)	Must only be saved on an approved council device Must be strongly encrypted. The password must be sent separately
Telephony (mobile and landline), Video Conference and Fax	Details of sensitive material should be kept to a minimum Can be spoken about over the telephone after validating the identity of the recipient of the information Faxes must only be sent to named recipients at a known fax number. Fax number must be confirmed and the recipient waiting to receive the fax. Fax cover sheet must

	be clearly marked OFFICIAL-SENSITIVE.
Disposal of paper documents	Shred document using a cross cut shredder
Disposal of digital equipment and media	See Secure Disposal or Re-use of Equipment

Personal responsibility

Staff, members and contractors are personally responsible for securely handling any information that is entrusted to them in accordance with this Policy.

Responsibilities

All staff shall ensure that:

- They recognise that all the information the Council owns is OFFICIAL;
- They recognise their personal responsibility in handling this data;
- They mark all OFFICIAL-SENSITIVE information they create;
- They handle OFFICIAL and OFFICIAL-SENSITIVE information in accordance with this Policy;
- They dispose of all printed material of a personal, confidential or sensitive nature, properly via the shredding and confidential waste bins provided by the Council. Where a contractor is requested to dispose of printed matter on the Council's behalf, they ensure that that contract with the Contractor contains appropriate conditions requiring the Contractor to dispose of the printed matter securely;
- They safeguard all personal and sensitive data by removing it from fax machines, printers, photocopiers and unattended areas, and data should be shredded where it cannot be attributed to a fellow member of staff;
- They do not open any correspondence clearly marked 'Restricted – Addressee Only' or 'Private & Confidential' and addressed by name, however they should take responsibility for ensuring it is forwarded direct to the named individual;
- Any information they handle is not saved to any PC or media outside of the Council;
- They inform the Data Security Group of the implementation of any new systems used to store information and data assets;
- They comply with the Data Protection Policy and if in doubt, do not store details of identifiable individuals on any computer;
- They report any instances where the Council's Data Management Policy has been or is being violated to the Data Security Group;

- They refer to the Data Security Group and/or Service Manager for guidance and authorisation if in doubt on any aspects of this policy.

System Procurement and Management

All new computer systems and hardware must be approved by ICT before they are purchased. This includes all software, hardware, online systems or hybrids of any kind. ICT will ensure that the system meets the Council's requirements; these include compatibility, Operating system and Database Support, system requirements and security. These requirements are maintained in a separate document entitled "Systems Procurement – Infrastructure Requirements". This document changes over time due to shifting supplier support and the constant change in the Information Technology landscape, however the following principles should always apply:

- Systems must run in a limited number of supported environments that can be supported properly;
- Any system must allow all security patches its environment requires to be loaded in a timely fashion;
- Systems with Web Components should support separation into a DMZ network to protect the core network. Web applications should be tested against all common attacks;
- Suppliers must urgently address security weaknesses found in their products;
- Products with known security weaknesses will not be deployed, and existing systems will be withdrawn from service until the flaw is fixed;
- The system shall support the Council's password policy;
- The system should provide auditing facilities relevant to the data and function of the system;
- No system shall be used which weakens existing security controls or allows them to be bypassed;
- Systems shall use strong encryption for the transfer of data;
- Vendors shall have strong security awareness and have written security policies. This is particularly important in remotely hosted solutions.

Vulnerability Management

ICT shall ensure it is aware of new vulnerabilities in its systems through vulnerability scanning, email subscriptions, websites and EMWARP membership. Where vulnerabilities can be addressed through patches these should be loaded as soon as appropriate testing can be completed. Where no patch exists ICT shall analyse the risk and take steps to mitigate the risk, this might be a workaround, blocking the threat in some other way, or in extreme cases disabling the system or software in question.

Security Testing

ICT shall annually commission a 3rd party specialist organisation to conduct security testing for internal and external vulnerability assessments. Automated vulnerability scanning software will also be used quarterly to provide additional information. Other vendor supplied tools will also be used to check the security of systems as required. These tools and their reports shall be protected so they may only be used by ICT staff.

The results of all these tests shall be used to continually improve the security of the network and individual systems.

Business Continuity Management & Risk

The Council has developed an IT Business Continuity Plan (BCP) which aims to counteract interruptions to normal Council activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

Overall maintenance of the Corporate BCP is the responsibility of the Service Manager of Audit and Risk Management. Each Service Manager should develop their own departmental BCP and work round manual procedures in the event of the loss of ICT systems/services.

This plan will be regularly tested and maintained.

Copies of the BCP have been circulated to key personnel and evacuation procedures are located on walls throughout Council Buildings. In the case of an emergency staff should contact their Line Manager or the Service Manager Audit and Risk Management - ext 3850.

Risk Management

Information risks are managed as part of the corporate risk register by the Audit and Risk Management team.

High level information risks are managed as part of the corporate risk register by the Audit and Risk Management team.

Detailed Risk Analysis including asset, threat, impact, likelihood and mitigation shall be carried out and documented by ICT Support. All new systems and any significant configuration change shall be assessed. Systems or changes which pose a significant risk, which cannot be mitigated or controlled, shall not be implemented. The Service Manager of Customer Services and ICT shall take the final decision.

Compliance

The Council will abide by all UK legislation and relevant legislation of the European Community relating to the holding and processing of information. This includes the following Acts and the guidance contained in the Information Commissioner's Codes of Practice:

- Computer Misuse Act 1990;
- Copyright Designs and Patents Act 1988;
- Data Protection Act 1998;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2005;
- Human Rights Act 1998; and
- Regulation of Investigatory Powers Act 2000.

More guidance on this legislation can be found on the Council's Intranet or by contacting the Legal Section.

The Council will also comply with all contractual requirements related to the holding and processing of information, including:

- The terms and conditions of licences and contracts; and
- The terms and conditions of authentication systems.

Public Services Network (PSN)

Public Services Network is a secure network interconnecting most Councils and many Government agencies. It is essential that the Council maintains this connection, particularly to support the Housing Benefit function. This connection will be replaced in time with the new Public Services Network connection (PSN) which serves a similar function.

Reference is made to Public Services Network throughout this document. Additionally, due to the special nature of this connect, the following rules apply:

- No Public Services Network services, such as email, file transfer and applications shall be used via any remote or mobile access system;
- Access will only be granted to those with a business need; and
- Users must sign a special form agreeing to the security rules for Public Services Network before they will be given access.

ICT will work to ensure compliance with the Public Services Network Code of Connection (CoCo), by showing a high standard of security compliance and continuous improvement.

PCI DSS

As the Council takes payment by card it must comply with relevant sections of the Payment Card Industry Data Security Standard.

Sensitive card data includes the full 16 digit Primary Account Number (PAN), the PIN and the verification code (from the back of the card). It is allowable to use the last 4 digits of PAN as long as the rest is not accessible by any means.

Due to the technical nature of the compliance process ICT oversees the process of becoming and retaining PCI DSS compliance. However all staff have a role in ensuring the Council is compliant.

Card Handling

All staff shall ensure that:

- They do not take any card payment details unless they are explicitly authorised to do so;
- They do not record or store any sensitive card holder data in any form, including, but not limited to:
    - Written on paper;
    - In an email, chat or text messaging systems;
    - In an electronic document such as Word, Excel, text file, Outlook note, sticky note, CSV file, image or screen dump, scan etc;
    - Database notes or other field entry;
    - As a filename;
    - In telephone calls (due to voice recording)
- Report any suspected payment card abuse to their Manager.

Staff authorised to take Card Payments shall ensure that:

- Card details are not stored by themselves or the Council as per the guidance above;
- Card details are only entered into approved systems which do not retain any sensitive data after authorisation;
- Card payment devices are only used in authorised locations and not moved without permission;
- Ensure only properly authorised service or repair personnel are allowed access to the device;
- Do not allow unauthorised changes or swaps of devices;
- Payment devices are only used for legitimate business use;
- Report suspicious activity to their Manager.

Managers involved in Card Payments shall ensure that:

- All staff are aware of their responsibilities with respect to card holder data and payment equipment and services;
- All systems and services involved in card payments are PCI DSS complaint and this is checked each year;
- Systems and Services are configured securely, see below;
- Terminals are inspected regularly, see below;
- Records are maintain of third party providers and what data is shared with them;
- Any incident involving card holder data is reported and handled using the normal Incident Reponses Procedure.

POS Terminal Configuration

Any member of staff configuring Terminals, Chip and PIN devices or other Point of Sale devices which take payment cards shall ensure that:

- The device is in a secure physical location which prevents tampering;
- All vendor supplied default passwords, or SNMP strings are changed;
- Unnecessary accounts or services are removed;
- Where applicable encryption keys are changed;
- Only secure technologies are used, e.g. not SSL or early TLS or insecure remote access implementations;
- Are far as is practical the system is locked down to prevent abuse;
- Wireless payment devices shall not be used without consulting ICT.

POS Terminal Inspection

In order to ensure that card payment devices are not tampered with.
Managers responsible for card payment devices must regularly check each device for:

- Additional devices plugged between the device and the network/phone line which may intercept card data;
- Tampering as indicated by damage to the case or additional attachments which it didn't have before;
- Changes in serial number, security labels, external marking or change of the colour of the case, all of which might suggest the unit has been substituted;

External Audit

Security testing is also provided by a 3rd party specialist, see Vulnerability Management.

Mapping Data

Mapping systems used by the Borough Council utilise data which is protected under copyright.

The Ordnance Survey data is strictly controlled by licence agreement, whether it is hard copy or electronic based. It is © Crown copyright and is only for internal business use. Unauthorised reproduction infringes Crown copyright and may lead to prosecution or civil proceedings. All other mapping and address data, including the Local Land and Property Gazetteer (LLPG) is controlled under licence agreement and is for internal business use only.

No data, whether it is hard copy or digital, is to be passed to persons or bodies outside the Council without the express written permission of the Council's Authority Liaison Officer and LLPG Custodian.

Privacy, Confidentiality and Monitoring

Privacy & Confidentiality

Users should note that no absolute guarantee of privacy can be given to the use of the Council's computer systems, including email, web, landline and mobile telephony, files or records of any kind. Operational requirements, such as actions to resolve system faults, data corruption, perform backups, remove spam or investigate complaints, may lead to systems administrators or managers being exposed to the content of systems, logs, emails, files, phone bills, SIM cards, phones etc. Where relevant, users affected by such events will be notified.

Content of logs may be examined during the course of properly authorised investigations into breaches of the Council's policies and procedures or the law, systems administration, fault finding or incident management.

Any information obtained by members of staff working in ICT during the course of systems administration (including monitoring) will be treated as confidential. However, users should note that where routine systems monitoring or administration indicates a breach of the Council's policies and procedures or the law, ICT will bring this information to the attention of the Council's relevant Corporate Director and/or the Council's Monitoring Officer and Chief Financial Officer.

Users should be aware that emails or other data may be accessed, on the authority of the user's manager or other authorised individuals, for the purposes of business continuity, or investigations into breaches of the Council's policies and procedures or the law.

Monitoring of Use

The Computer Systems are installed expressly for the purpose of supporting the Council's business. Users must have no expectation of privacy in anything they create, store, send or receive on the Council's systems. Users' access can be monitored without prior notification if the Council deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, the Council reserves the right to take disciplinary action, including termination of employment and/or legal action where appropriate.

ICT keeps records in order to monitor traffic, system usage, calls, texts, web use, file transfer, removable media use, and emails. These include the usernames, dates, times, and details of all access. These logs are kept for at least 6 months and secured against unauthorised access. ICT shall ensure device clocks are synchronised with a trusted time source.

To maintain security and integrity, the Council reserves the right to investigate, review data and monitor logs in a number of circumstances, including but not limited to, where:

- A virus is threatening the functioning of the Council's ICT assets or is likely to delete or corrupt user data. Logs may be examined in order to identify and delete the offending material;
- There is a suspicion that the Council's ICT assets have been misused or that this policy which governs the use of the computer systems has been contravened;
- The police request this, and where it has been established that such cooperation with the police is in direct furtherance of a criminal investigation;
- It is to prevent unauthorised access to Council systems;
- It is to detect unusual trends in use of services;
- It is to ascertain or demonstrate standards which ought to be achieved by those using the facilities;
- It is to prevent or detect crime;
- It is to ensure effective operation of the facilities;
- It is to establish the existence of facts relevant to the business;
- It is to determine if communications are relevant to the business - for example where an employee is on sick leave or on holiday.

Users should be aware that it is not possible to differentiate between business and personal use. All usage may be subject to monitoring.

Information obtained through any monitoring will not be used for any purpose other than that for which it was collected unless such monitoring reveals activity of a nature that no responsible employer could reasonably ignore.

In using the Council's computer facilities users accept all the relevant policies, protocols and procedures relating to their usage. Consequently, users agree to a right to inspection of users' usage of the Council's ICT assets by ICT and Internal Audit staff under the circumstances explained above.

The rights of employees under the Data Protection Act 1998 and the Human Rights Act 1998 are not affected.

Document Attributes

Document Information

Title	**Information Security Policy**
Description	The objectives of this Policy are as follows: - • To ensure that the Council's ICT assets are protected against theft, loss, damage, corruption and any unauthorised actions; • To ensure that employees and members are aware of the risks to which ICT systems may be subjected and of their responsibilities to minimise those risks; and • To ensure that the Council complies with the many and varied laws surrounding Information and communications.
Author	ICT Technical Manager (collating existing documents)
Date Created	August 2012
Last Review Date	
Next Review Date	

Document History

Date	**Summary of Changes**	**Version**
August 2012	1st Draft, Prepared by Gary Bennett	1.0
Sept 2012	2nd Draft, proof read and edited by Helen Barrington, Vince Rimmington and John Staniland	1.1
October 2012	3rd Draft, final amendments by DSG prior to SLT	1.2
November 2012	4th draft incorporating amendments by SLT	1.3
February 2013	Amendments following Service Manager Consultation, initial published policy. Classification changed to UNCLASSFIED	1.4
August 2015	Removed UNCLASSIFIED classification Large update to PCI DSS section regarding Payment Card handling Added wireless networking section Changed references to Government Connect to Public Services Network Small updating changes, job titles, removing unneeded lines. Added two factor requirement to OWA	1.5

Document Approval

Date	Job Title of Approver(s)	Version
6/1/2013	Data Security Group	1.4
12/3/2013	Senior Leadership Team	1.4
4/4/2013	Cabinet	1.4

Distribution

Name / Group
ICT Section
All Employees via email
All Members via email