B

CPR.32 15/16

Corporate Policy and Resources Committee

Date: 10 November 2015

Subject: Bring Your Own Device Policy

Report by:	Director of Resources
Contact Officer:	Steve Anderson Information Governance Officer 01427 676652 Steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	The purpose of this report is to introduce a new council policy on the authorisation and use of privately-owned devices to access authority information assets.

RECOMMENDATIONS:

1) That members approve and formally adopt the Bring Your Own Device Policy.

2) That delegated authority be granted to the Senior Information Risk Owner (SIRO) (Director of Resources) to make minor house-keeping amendments to the policy in the future, in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.

3) That on approval of the Policy relevant policy statements are communicated to all staff in accordance with Approved Code of Practice (ACoP) 19 – Application of Information Policies, and to members in a format to be agreed .

IMPLICATIONS

Legal: This report has direct positive implications on the council's compliance with legislation including, but not limited to, the Data Protection Act 1998. Specifically, the implementation of this policy will:

1. Prevent access to council data from non-council-owned mobile devices which have not been approved and configured for the purpose; and

2. Help to safeguard council data accessed from a privately-owned mobile device that has been approved and configured for the purpose.

Financial: There is a budgeted allowance of £500 per member towards the cost of their preferred privately-owned mobile device. There are no proposals to fund devices for staff or others.

Fin Ref: FIN/77/16

Staffing : None from this report

Equality and Diversity including Human Rights: None from this report

Risk Assessment: None

Climate Related Risks and Opportunities : None from this report.

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)	**Yes**	□	**No**	**X**

Key Decision:

A matter which affects two or more wards, or has significant financial implications	**Yes**	□	**No**	**X**

Background

1.1 The council is committed to flexible working and provides staff with tablet computers and smartphones to enable them to work from a variety of locations and at hours to suit their personal circumstances. The council recognises that some staff want to use their own mobile devices ("Bring Your Own Device" (BYOD)) to access council applications to rationalise the number of devices they need to carry. Elected members are given an allowance to purchase devices of their choice to carry out their council business and these devices may be permitted to access council services such as email. However, the council also recognises that BYOD raises a number of information security and data protection concerns because the device is owned and managed by the user rather than the council.

1.2 The Mobile Device Audit 2015 recommended that the council implement a BYOD Policy to support the council's existing Flexible Working, Remote Access, and Mobile Device policies. This report introduces a new BYOD Policy to set out the framework in which a BYOD service is to be implemented and operated. The new policy will be incorporated into the Information Security Policy Framework.

2. Scope

2.1 The policy applies to staff, elected members, co-opted members, contractors and third parties who wish to connect to any of the council's computer systems to access council data using a personal device.

3. The Policy

The BYOD Policy sets out the council's rules with respect to:

1. the technical solution for BYOD and the security controls required;
2. the devices that may be approved for connection;
3. the approval and access provision processes;
4. the council's responsibilities;
5. the user's responsibilities;
6. actions in the event of a security incident (i.e. a user-owned device is stolen);
7. acceptable use of a BYOD service; and
8. policy compliance.

4. **Policy Consultation**

The policy has been developed in consultation with the ICT Manager; the Corporate Leadership Team; and staff, unions and elected members through the Joint Staff Consultative Committee. All the above consultees have recommended the policy for formal adoption.

During the Corporate Policy and Resources Chairman's Briefing a concern was raised regarding the amount of data that would be wiped should the device be lost or stolen. If the council's policy was to perform a complete wipe of the device in the event of a security incident then this was considered to be unacceptable. It was agreed, therefore, that the policy would be amended to reflect that Mobile Device Management software will be deployed and configured on devices to permit a "selective wipe" of council data only, leaving user data such as personal documents and photographs intact.

5. **Policy Implementation**

Due to the policy setting out both the technical controls needed to comply with legislation and the user responsibilities in one document, and the low take-up expected, it is not considered appropriate to issue the policy to all staff and members. Instead, we will communicate the policy statements relevant to staff and members and those relevant to managers and technical staff in different formats in accordance with Approved Code of Practice (ACoP) 19 – Application of Information Policies (Appendix 2). This is the approach we intend to take with all new and revised information policies in the future.

Since it is likely that the majority of users of the BYOD service will be elected members because of the members' ICT allowance scheme, the policy messages and implications will be communicated to members in a format to be agreed.

6. **Decisions Required**

1) That members approve and formally adopt the Bring Your Own Device Policy.

2) That delegated authority be granted to the Senior Information Risk Owner (SIRO) (Director of Resources) to make minor house-keeping amendments to the policy in the future, in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.

3) That on approval of the Policy relevant policy messages and implications are communicated to all staff in accordance with Approved Code of Practice (ACoP) 19 – Application of Information Policies, and to members in a format to be agreed.

7. **Appendices**

Appendix 1. Bring Your Own Device Policy
Appendix 2. ACoP 19 – Application of Information Policies.

Bring Your Own Device Policy

Table of Contents

1. Overview

The council is committed to flexible working and has a suite of flexible working policies and associated guidance and toolkits. Furthermore, the council recognises that device owners wish to use their own mobile devices ("Bring Your Own Device" (BYOD)) to access council data and use council applications as part of flexible working arrangements.

Principle 7 of the Data Protection Act 1998 (DPA) states that "appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data." BYOD raises a number of information security and data protection concerns because the device is owned by the user rather than the data controller (the council).

It is crucial that the data controller ensures that all processing of personal data which is under his control remains in compliance with the DPA and other regulatory or partnership requirements.

The council must consider how to protect its data in the event of loss or theft of a device which it does not own or is able to fully-manage.

The council must also remain mindful of the personal usage of such devices and ensure that technical and organisational controls used to protect the council's personal data remain proportionate to and justified by the real benefits that will be delivered.

The device owner must be aware that a certain level of control over their device will be applied by the council for as long as access to council data is permitted. This will normally only extend to the enforcement of a strong password or pin and a defined lock-screen period but could include, in some circumstances, the requirement for particular versions of operating systems and applications or the need to "selectively wipe" a device to remove council data. A selective wipe will remove council data such as council emails and calendar appointments but will leave user data such as documents and photographs intact.

Access to and continued use of network services is granted on the condition that each device owner reads, signs, respects and follows the council's policies concerning use of these devices and services. The use of a personally-owned device in connection with council business is a privilege granted to device owners through approval of their line manager, People and Organisational Development, and the ICT Department. The council reserves the right to withdraw these privileges in the event that device owners do not abide by the policies and procedures set out in this document.

2. Purpose

This policy outlines the responsibilities of both the device owner and the council with regard to BYOD.

The document sets out the council's policy for protecting the corporate network from data leakage to unmanaged personal devices. It also provides standards and guidance for acceptable behaviour for the use of personal devices such as smart phones and tablets by the device owners to access network resources, namely their council e-mail and calendar, for business purposes. This policy will be updated regularly to accurately reflect devices and the services provided.

3. Scope

This policy applies to employees, elected members, co-opted members, contractors and third parties who wish to connect to any of the council's computer systems to access council data using a personal device. Third parties would additionally be required to sign an appropriate data sharing agreement or contract.

Current devices approved for BYOD use are listed below along with the minimum system requirements:

- Manufacturer supported Android Smart Phones and Tablets
- Manufacturer supported iOS iPhones and iPads
- Manufacture supported Windows Mobile

Devices below these specifications will not comply with our policies and therefore will not be supported.

4 Policy

4.1 What is BYOD?

BYOD refers to organisations permitting their staff and elected members, co-opted members, contractors and third parties to bring personally owned mobile devices (e.g. tablets and smart phones) to their workplace, and use those devices to access privileged organisational information and applications.

4.2 Who manages this service?

The ICT Department in conjunction with People and Organisational Development and Corporate Governance will manage the BYOD service on behalf of the council. In specific terms the BYOD service includes the technical controls, approval, monitoring, reporting and security incident processes, (e.g. wiping council data from the device) for all user-owned devices.

4.3 What support will the council provide?

The council will not support or maintain any personal mobile device. Furthermore, the council will not cover any damage to the device and recommends that device owners insure their device as part of their home contents insurance and advise their insurer that the device will be used for work purposes at home and at work locations.

On approval of the application the ICT department will install mobile device management software free of charge. This will enable the device owner to connect to the council's approved access gateway to access their council e-mail and calendar and any future services that may be provided. However, the council will not reimburse users for the acquisition of the device, its use, maintenance or replacement, or any carrier service charges incurred. To be allowed access to the council services provided by the BYOD service the device owner must agree to all terms and conditions in this policy.

Device owners whose devices do not meet the council's standard approved device requirements will not be allowed to access the service. Owners of personal devices are not permitted to connect to the council infrastructure without documented consent from their line manager and the ICT Department. Furthermore, the council and the ICT Department specifically reserve the right to disable or disconnect some or all services without prior notification.

4.4 The Council's Responsibilities

4.4.1 Risk Management

As the data controller, the council is responsible for ensuring that all processing for personal data which is under its control remains in compliance with the Data Protection Act 1998. The council must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect council-owned data must remain proportionate to the risks.

A risk-based decision to deploy a BYOD service will look at both risks and opportunities as part of the decision process. Consequently, the council will need to consider the following:

- what type of data is held;
- where data may be stored;
- how it is transferred;
- potential for data leakage;
- blurring of personal and business use;
- the device's security capacities;
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device.

4.4.2 Technical Controls

The most significant risk posed by BYOD is data leaking from the secure corporate network to unmanaged, non-council-owned devices. To prevent this the council will:

1. Deploy a "walled-garden" security architecture.
2. Quarantine devices before access is given.
3. Install an appropriate Mobile Management client
4. Encrypt communication over public networks using SSL technology.
5. Enforce a strong password policy onto devices.
6. Enforce device encryption on devices that support this.
7. Monitor access logs and report inappropriate or insecure behaviour.
8. Continuously review and improve technical policies deployed on devices.
9. Subject the BYOD solution to the council's annual penetration testing.

4.5 Device Owner Responsibilities

The device owner has specific responsibilities, as listed below:

- The owner will not lend anyone (including family members) the device to access council information or use the council infrastructure.
- Should the owner decide to sell, recycle, give or change the device, they will inform the ICT Department Service Desk by phone on 01427 675165 as soon as possible.
- The policy will require a 6 digit pin to access the device. The device or application will lock every 1 minutes of inactivity requiring re-entry of the pin.
- In order to access an Outlook mailbox or calendar, the owner will need to periodically enter their network account password. This rotates every 90 days, as per the network domain policy.
- The device owner is responsible for backing up their personal files.
- Device owners MUST NOT send personal information owned by the council from their own personal device.
- Owners must ensure that their device is compliant and that security software is kept up to date. The system will check whether your device meets compliance criteria and if not, will automatically stop syncing.
- A device will be selectively wiped (council data only) without notice if: (a) the device is lost; (b) the owner's employment with the council is terminated; or (c) the ICT Department detects a data or policy breach or virus.
- In addition to the above security settings, all users are expected to use their device in an ethical manner. Using a device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jailbreaking" an iPhone or "rooting" an android device. Owners should be aware that Jailbroken or Rooted devices will not be permitted as it violates the device compliance element of this policy. Any devices that become rooted or jail broken will stop syncing and will be reported to the ICT Department.
- When device owners leave the employment of the council their access to the council infrastructure and applications will cease and their device will be de-provisioned as part of the leaver's process to ensure access to council data is ceased and council data is wiped from the device.

4.6 Security Incidents

A number of security incidents could occur when using personal devices with council data. These include:

- theft or loss of data or any equipment;
- transfer/disclosure of sensitive data to those who are not entitled to receive it;
- compromised passwords;
- attempt (either failed or successful) to gain unauthorised access to data or systems;
- connection of equipment that has either not been approved by the council;
- non-compliance with council information security policies and associated procedures including this policy;
- hacking attempts, virus attacks, phishing etc.;
- device "jailbreaking," "rooting," or the equivalent; and
- making any other modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator.

Performing such actions or making such unauthorised modifications is essentially an “inside attack” on device, application, and data security, and should be treated very seriously.

4.6.1 If a security incident should occur

If a security incident should occur, e.g. a device is lost or stolen or is infected with malware, the device owner is required to inform the ICT Department Service Desk immediately with details. The ICT Department is to raise a security incident in accordance with the Information Security Incident Management Policy.

The ICT Department reserves the right to selectively wipe council data and applications, if it is deemed necessary. This should not impact other applications and data, such as the native Address Book data and any personal files on the device.

4.7 What is the procedure for accessing this service?

4.7.1 Approval Process

- The device owner and user will raise a Systems Access Form through the ICT Service Desk.
- The device owner will read this policy and sign and date Appendix 1.
- The device owner’s line manager will approve the application by counter-signing Appendix 1.
- The signed Appendix 1 is to be scanned and an electronic copy e-mailed to ICT.

4.7.2 Access Provision

- On receipt of the signed policy statement, ICT will make an appointment with the device owner to enable the mobile device management software on the device.
- From the date of receipt of the signed policy statement, the anticipated time for this activity is approximately one work week.

4.8 Acceptable use of the BYOD service

Device owners are expected to behave in accordance with the council’s Officer Code of Conduct at all times whilst undertaking work for the council. Examples of behaviours covered by the Officer Code of Contact that are relevant to BYOD include the use of email, confidentiality, and the use of social media. Further information can be found on Minerva, from line managers, or by contacting a People and Organisational Development Advisor.

Device owners should be aware that any personal device used at work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against the council. The owner’s personal data could be examined not only by the council but also by other parties in any lawsuit.

4.9 The Council's Release of Liability and Disclaimer Statement

The council hereby acknowledges that the use of a personal device in connection with council business carries specific risks for which the device owner and user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

The council hereby disclaims liability for the loss of any such data and/or for service interruptions. The council expressly reserves the right to wipe the device management application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining the council's infrastructure and services.

The council also disclaims liability for device owner injuries such as repetitive stress injuries developed. The council provides IT equipment that is suitable for long-term office use.

Device owners bring their devices to use at the council at their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

The council is in no way responsible for:

- Personal devices that are broken while at work or during work-sponsored activities;
- Personal devices that are lost or stolen at work or whilst undertaking work-related activities;
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)
- The management or creation of users own 'cloud' based user accounts, which are required for purchasing software, or backing up data

The council does not guarantee that the service will be compatible with the owner's equipment, or warrant that the service will be available at all times, uninterrupted, error-free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best service it can.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. The device owner is responsible for confirming any impact on rates as a result of the use of council supplied applications and will not be reimbursed by the council.

Finally, the council reserves the right, at its own discretion, to remove any council supplied applications from a personal device as a result of an actual or deemed violation of the council's BYOD Policy.

5 Policy Compliance

5.1 Compliance Measurement

The ICT Department and the Corporate Information Governance Group will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Senior Information Risk Owner (SIRO) in advance.

5.3 Non-Compliance

Breach of this policy by a council employee may lead to disciplinary action which could result in dismissal, suspension or termination of access to the service and/or prosecution and/or the council co-operating with law enforcement organisations, government agencies, other legal authorities or third parties involved in the investigation of any suspected or alleged criminal or civil offence. Please refer to the disciplinary policy and procedure for more information.

A complaint made against a councillor under this policy should be referred to the Monitoring Officer who will advise on the appropriate action to take.

5.4 Policy Review

This policy will be reviewed as and when required and at least biennially.

6 Related Standards, Policies, and Processes

The following documents are related to this policy and should be referred to where appropriate:

- Data Protection Policy
- Data Protection Breach Policy
- Information Security Policy
- Remote Working Policy
- Mobile Device Policy
- Social Media Policy
- Email Policy
- Information Security Incident Management Policy

Appendix 1 - Bring Your Own Device Application Form and Acceptable Use Statement

Please return a signed copy of appendix 1 to the ICT Service Desk.

User Application

I, ____________________________, the device owner and user, request permission to use my_________________________ to access council data and use council applications as part of flexible working arrangements. I confirm that my device is running on version ____________ and meets the minimum system requirement listed in this document.

I have read, understood and agree to respect and follows the council's policies concerning acceptable use of these devices and services, as documented in the Bring Your Own Device Policy. Further, I have understood the limitations of this IT Service and the consequences of misuse on my behalf.

__________________ ________________________ _____________

Name of User Signature Date

Line Manager Approval

__________________ ________________________ _____________

Name of Line Manager Signature Date

For use by the ICT Service Desk

CRF No.: ______________

Date Signed Form returned to Information Services: ______________

Date Mobile Device Management enabled: ______________

You must read, understand and formally accept this policy by signing and returning the Bring Your Own Device Application Form before you can access the council's computer systems using a personal device. You may be asked to re-confirm acceptance annually with updates being sent out throughout the year.

WEST LINDSEY DISTRICT COUNCIL ACoP

Approved Code of Practice No. 19 – Implementation of Information Policy Documents

1. Detail of the Process/Function

Information policy documents are written to address the specific risks to an organisation when creating and processing information. Policies set out how the authority will mitigate these risks in order to comply with relevant legislation, standards, and best practice when managing, processing, and protecting OFFICIAL information. They provide the set of rules on which processes, procedures, guidance, and training must be based.

This ACoP details how Information policy documents will be approved, implemented, communicated to users and monitored for effectiveness, and how they will be reviewed and maintained.

The Information Governance Officer (IGO) is responsible to the Senior Information Risk Owner (SIRO) for implementing and monitoring the effectiveness of the council's Information Management and Security Policy Frameworks which are elements of the Information Governance Framework.

2. Scope of the ACoP (what it does or does not cover)

This ACoP covers the creation, consultation, approval and maintenance of the council's information policy documents. The ACoP also details the communication, monitoring, and training that will be provided to staff, councillors, partners, and third parties to whom the policy is applicable.

3. Describe in more detail the Process/Function

a. **Policy Creation, Consultation, Approval, and Maintenance.** Information policy documents are components of the Information Governance Framework and will be created and maintained by the IGO. A recommendation for formal adoption of a policy document by the council is required from the Corporate Leadership Team (CLT) and from staff and unions through the Joint Staff Consultative Committee (JSCC). The Corporate Policy and Resources Committee (CPR) approves the policy document for adoption. Information policy documents are generally reviewed annually and delegated powers for minor changes can be granted to the SIRO in consultation with the Chairmen of the JSCC and CPR committees.

b. **Communication**. Following formal adoption by the CPR Committee, the IGO must publish the document in the Corporate Information Policy Library and present the content of the policy to the Wider Leadership Team (WLT). The WLT agenda item must be booked in advance on the Forward Plan to ensure that the policy is communicated as quickly as possible. WLT members should cascade the policy to their teams through team meetings and briefings and may invite the IGO to attend and discuss the policy with their teams if required. The IGO will prepare and publish a “Clarity” article on Minerva explaining the key policy messages, and what they mean to the council and to its elected members, staff, partners, and third-parties in clear, plain English.

c. **Monitoring of Policy Effectiveness.** The following key dimensions of information security are recognised as being useful when determining the metrics needed to assess the strength of an organisation’s security posture and, by definition, it’s information policy effectiveness:

- **Uptime:** The ability to withstand cyber-attacks and avoid costly business disruption.
- **Compliance:** The ability to achieve compliance with all applicable regulations and laws.
- **Threat containment:** The ability to prevent or quickly detect external security threats such as cybercrime, social engineering or malicious attacks.
- **Cost efficiency:** The ability to manage investments in information security and data protection in a competent (non-wasteful) manner.
- **Data breach prevention:** The ability to prevent or quickly detect internal security threats such as the negligent or incompetent insider.
- **Policy enforcement:** The ability to monitor and strictly enforce compliance with internal policies, procedures and other security requirements.

In addition to applying and monitoring metrics, regular analysis and response to information security incident findings and recommendations is to be carried out by the CIGG and fed into the council’s policy where possible.

d. **Training.** The IGO will ensure that internal information awareness training is reviewed and updated as and when information policies are published or amended. Changes to training are to be communicated in “Clarity” articles on Minerva.

4. Who does this ACoP apply to?

a. **Senior Information Risk Owner (SIRO)**. The SIRO is responsible for the council’s policy with regard to the risks to its information.

b. **Information Governance Officer.** The IGO is responsible for drafting information policy on behalf of the ICT Manager and managing the consultation and approval process through to formal adoption by the Corporate Policy and Resources Committee. The IGO is also responsible for communicating, monitoring, and reporting policy effectiveness through the Corporate Information Governance Group (CIGG) to the SIRO.

c. **ICT Manager.** The ICT Manager is responsible for ensuring that security measures commensurate with the council’s information policies are applied to the corporate ICT infrastructure, systems, and devices and that these measures meet (or exceed) legislative, recognised standards, accepted best practice, and any other relevant requirements. The ICT Manager is also responsible for making sure that effective training is delivered to users where the policy specifically requires it, for reacting to changing and emerging threats, and for applying technology and security updates in a timely manner.

d. **The Corporate Policy and Resources Committee (CPR).** The CPR Committee is responsible for formally approving new and amended corporate council policy.

e. **The Joint Staff Consultative Committee (JSCC).** The JSCC is the council's consultative body comprising elected members, representatives from union members and non-union staff, and supported by senior management. The JSCC is responsible for making sure new and amended policy complies with employment law and codes of conduct and recommends new and amended corporate policy to the CPR Committee for adoption by the council.

f. **The Corporate Information Governance Group (CIGG)**. The CIGG is responsible for reviewing information policy and providing recommendations and comments to the IGO. The CIGG is also responsible for cascading information policy to their departments/teams and for bringing comments and issues from their departments/teams for discussion at group meetings.

g. **Users.** All staff, councillors and third parties who have been authorised to access OFFICIAL information using corporate facilities and equipment are responsible for complying with the information policies relevant to their role and the training and guidance provided by the ICT Department.

5. Signatories

This ACOP has been signed by the officers detailed below as responsible senior officers who are accountable for ensuring this procedure is followed.

Job Role	**Name**	**Signature**	**Date**