Agenda Item 6

Digital Strategy – Principles and Resources

Agenda Item 6

Falkirk Council

Title:	**Digital Strategy – Principles and Resources**
Meeting:	**Executive**
Date:	**14 May 2019**
Submitted By:	**Director of Corporate and Housing Services**

1. Purpose of Report

1.1 The purpose of this report is to advise Members of the digital strategy for the Council and the principles that underpin this, along with key areas for action and the commitment and resources required to deliver on our ambitions.

1.2 The digital strategy is a key component of the Council's business plan and will help shape how we transform our services over the next five years.

2. Recommendations

2.1 **The Executive is asked to:-**

(1) Note the digital strategy set out in appendix one.
(2) Agree the actions we will develop over the coming months and years to deliver us as a digital council –set out in para 3.3 – 3.5 of appendix one
(3) Approve the Information Security Policy and Acceptable Use policies attached and over the coming months these are rolled out across the Council to employees and Members.
(4) Note ongoing engagement will help identify the future digital requirement of our Council Services; and
(5) Note that this Strategy will support the delivery of the digital requirement set out in the Council's five-year business plan.

3. Background

3.1 The way the Council delivers its services is changing. This change is being prompted by reducing resources, opportunities opened up by technology and, importantly, by the changing expectations our customers, services and elected members have on the services we deliver and the way these are delivered. We have, over the last number of years, significantly changed the way we deliver technology that supports our business. We have moved to a more mobile and flexible platform that allows people to access their systems etc., out with their offices. We are in the process of replacing all our telephony to ensure this offers more flexibility and functionality. We have redeveloped our website and offer more and more services online. Services are using technology to offer a better service to customers in areas such as BMD, home care etc. We offer very different ways to teach and learn through the deployment and use of technology.

3.2 This work has allowed us now to think where we want to go and how we achieve this in a planned, safe and flexible way.

3.3 We have also been engaging with the Local Government Digital Office on a range of projects that are happening across Scotland and using learning in other authorities to critically review our offering and support to services. This has led to a self assessment on our digital maturity, a review of our approach to digital services and importantly questioning fundamentally our ambitions to become a digital council, i.e. one that thinks digital first and by design.

3.4 We have therefore spent some time reflecting on the feedback from the digital maturity assessment, the feedback from employees from the COTF listening events and are proposing a way forward with regards to our digital strategy. This digital strategy sets out the need for change, the three core elements of that strategy and what we need to do in high level terms to take forward this strategy. The strategy is appendix one of this report.

3.5 Audit Scotland published a report in May 2017 that outlines the principles for a digital future. This report was published in response to lessons learnt from public sector ICT projects and to promote effective delivery for investment. The report does not provide a check list but rather provides themes based on core principles that public sector organisations are urged to take account of. These include individual projects set within a central framework for oversight and assurance:

- Comprehensive planning – setting out what you want to achieve and how you will achieve this
- Active governance – ensuring appropriate oversight and control
- Users being at the heart of change
- Clear leadership that sets the tone and culture but also provides accountability

4. The Strategy

4.1 The strategy has significant and profound consequences for the way all Services design and deliver services. It challenges the role of leaders not just to support change but actively to lead transformation across the authority but importantly within their services. As such it sets a direction with underpinning principles at this stage. Detailed actions on specific work will be subject to further discussion with services and developed over the life of the strategy.

4.2 The strategy is set out in appendix one of this report.

4.3 At the heart of our digital strategy is service redesign, based on the needs and perspective of the customer. This approach changes the focus from what we, as an organisation think we should be delivering, to what our customers' problems are and how we can we resolve these. This redesign means moving away from purchasing an item of software that we think might solve an internal problem we have, to engage with customers and stakeholders on what the services they receive should look like and then making sure the technology supports that. This should give us better value in terms of change making a real difference, ensure we are not purchasing technology that does not add value and also begin to make ensure we know our customers needs by actively and consistently engaging with them.

4.4 However, the strategy also gives significant challenge to the way we support the Council in technology terms. As such we will have on going discussions with Services on the consequences of this and how we can best support them going forward. We will also engage further with the Local Government Digital Office on the support they can give us to move from where we are to where we want to be as an organisation, and with various elements of the strategy.

4.5 There are clear benefits to adopting the strategy and setting on a clear course to deliver digital transformation through service redesign based on the Scottish Design Principles and underpinned by a robust technology platform. The benefits for the Council include:

- More customer focussed services delivered by technology and driven by data.
- The ability to manage contracts and service delivery more closely and timeously to ensure compliance and consistency thus reducing costs.
- Delivering savings through retiring legacy systems and sweating our technology platform and software.
- Services being consistently delivered to customers and staff – across service thus improving customer and staff experience.
- Eliminating waste and making processes more efficient, effective and reducing duplication.
- Enhancing jobs by reducing repetitive tasks.
- Significant savings being able to be identified in conjunction with services as the model of transformation rolls out.
- Ensuring our platform for service delivery and customer information is safe, secure and managed effectively.

4.6 The specific benefits to services will be quantified as we take the strategy forward. We do anticipate if we adopt this approach we will support services to deliver on customer expectations, adopt technology that supports that change, reduce work at the back office and for customers and reduce the number of systems across the Council. We know through the contact centre what services people are requesting, complaining about and where efficiencies can be made. We will work with services to agree where our efforts will be directed to deliver maximum benefit.

4.7 While not pre empting work with services there are clear areas where this work might have benefits including:

- Housing allocations –making it easier to bid for a house from a customers perspective
- Allowing parents to manage pupils payments, activities etc
- Registration and licencing services - as these services are centralised how we can support people to self serve where appropriate to do so. This means our limited resources being available to those who need more support
- Further developing applications for waste services.
- Planning applications – how we can support the service to streamline this process and potentially reduce costs
- Automation of processes within Revenue and Benefits using Artificial Intelligence.
- Streamlining HR and Payroll processes.

- Service desk – how we can review our support for technology that meets the changing needs of the business including support for teachers and pupils.

4.8 It must be stressed that these are only examples of areas we can work with services to examine. We will also work with services to ensure they are sighted on work within other Councils, through the LGDO, that they might look to take forward within the Council.

5. Moving Forward

Resourcing a Digital Council

5.1 The existing technology strategy set out a robust governance structure that has been superseded by our approach to Council of the Future. Our digital strategy will be an integral part of that governance, ensuring that we have a single approach to the deployment of technology across the Council and that single approach is taken by all Services. This will mean extending our approach to budget consolidation, ensuring a robust commitment to corporate implementation and use of systems, software, data and infrastructure.

5.2 The commitment to centralising all technology budgets was agreed in the last technology strategy and will now be implemented. The reason for the delay was the lack of governance that would allow decisions to be taken centrally but fully informed by Service needs. The Council of the Future governance gives us that framework. Work has therefore started to identify all budgets / spend with a view to having a centralised IT budget from the beginning of the next financial year i.e. 20/21. This centralisation allows us to manage our limited support resource but also to ensure consistency of approach to technology across the Council. This centralisation is necessary irrespective of the decisions surrounding the emerging digital strategy, but do underpin and support the new way forward.

5.3 We have also been working with the Local Government Digital Office to look at the Scottish Government Digital First Service Standard. This gives us a core set of questions to assess our approach to technology and indeed our spend on that. It allows projects to be assessed against 22 criteria that include issues such as user research, content design, product assessment, technical specification etc. While the Government's approach is too resource intensive, there are discussions about developing a digital service standard light for local government. It is this standard that we hope to use to assess projects and spend that we will progress as a council. Until this is developed we will develop with Services a check list of criteria for projects that involve technology in order to ensure alignment to our emerging digital strategy. This will complement the use of the Scottish Design Standards in terms of green lighting projects for development and spend.

5.4 With regard to our approach as a Council, we are at the point that we must take decisions that reflect our transformation ambitions. While we have built solid foundations for a Digital Council, we cannot continue with the resources we have to support digital services nor our technology foundations. While the Council has reflected its ambitions within its capital programme, we are limited in our capacity to deliver on this.

5.5 To date we have relied on upskilling existing staff to deliver on more complex and core initiatives that will provide the foundation for the Council providing services to communities in the future. This is at the same time as maintaining and supporting our existing and growing technology estate such as network and software.

5.6 When we are working with services we are uncovering significant issues of process redesign that gives significantly more work to officers in the journey to streamline effective digital services. We are also encountering problems of user acceptance testing capacity, lack of focus on delivery while at the same time we have an ever increasing IT estate that we need to support. We cannot deliver change while at the same time keep the lights on with the resources we have.

5.7 We also do not have the skills we need in some critical areas e.g. user researcher etc., and therefore need to enhance our capacity and develop new skills in service design. We are looking to explore Dundee City Council's approach to services redesign as being at the core of this approach. This work will be the foundation for changing the way we design or indeed redesign our services.

Transformation by Redesign

5.8 To deliver the ambitions of the council we need to ensure that we are resourcing the support that will deliver on the changes we need. If we are to be a Digital Council then firstly we must invest in the teams currently delivering in key areas namely our web and digital services and improvement teams. We must also seek to resource training. To achieve a successful outcome, additional staffing will be required, as clearly identified via the Digital Maturity assessment.

5.9 As the web site is becoming more important as a primary means of accessing services, there are significant risks for the Council if we do not maintain and resource this platform appropriately. At the moment we are spending time updating and maintaining our current on line platform. This leaves little time for further development. We therefore need to create capacity for maintenance while at the same time picking up the pace with our digital transformation of critical services.

5.10 Key to the service design approach is the initial engagement with customers and services. We will establish capacity to work with all parties to understand their needs and use design principles to shape services so that they work for the people that are using them.

5.11 Quality control is key to ensuring a consistent experience for customers and it is a resource which is unfortunately limited within our teams and is a challenge to find within our services. In adopting the service design principles, consistency is paramount in our approach. A quality control resource is therefore required to undertake the quality control checks for all newly developed systems.

5.12 In addition to this, the principles will be further embedded by work on a pilot service design project, supported by external service design experts. This will be achieved by establishing a six-week project to design a discrete area of service in accordance with service design principles. Up to 10 Council officers would support this exercise, drawn from the service area itself, Policy, Technology and Improvement and the PMO. The proposal is that they would potentially be assigned to the project for e.g. two days a week, and would learn hands-on service design skills that can be applied widely across the Council. The output of this would be a case study and a consistent methodology.

5.13 To deliver the change reflected in the strategy, the Council of the Future Board has allocated some of the transformation funding to take this forward. This will give some capacity to start this work but there will have to be decisions taken as we move forward on the capacity to support this through mainstream resources.

5.14 Over the coming year, we also need to review our research and innovation capacity within the improvement team. At the moment that team is focused on delivering some of our significant technology projects rather than looking at where the Council needs to be in the future, particularly around areas such as AI, the internet of things, the virtual classroom etc. In addition to making sure our core foundations are supporting the Services we require. If we are to continue to develop and use technology then we must ensure we have the resource to not only do the horizon scanning but then to work with services through to implementation. This capacity should make sure we are maximising the investment the Council makes in technology by ensuring consistency of application across the Council and also we are only buying systems that meet our agreed standards.

Rock Solid Technology

5.15 To achieve our aspirations and ensure solid technology foundations for a digital council, there are a number of steps we need to take. We will over the coming year provide additional tools and systems that will allow services and employees to work differently. This change through moving to Office365 builds on work currently taking place in our schools and seek to increase collaboration, communication and improve how we manage information. It will seek to start moving from an internal data centre or server room to externally hosted systems and data.

Building a Robust Infrastructure

5.16 Services understand that the significant increase in the use and spend on technology across the Council has not been mirrored in an increase in support of that very same estate. Thus while we are increasing the number of users, equipment and systems the Council relies on deliver services and achieve savings, we have over a number of years reduced the capacity to support, maintain and care for our network, systems and infrastructure. This is also limiting our capacity to deliver on significant change. One example is that we currently have been delivering changes in our network, seeking to increase our WIFI capacity, moving all of our telecoms and upgrading servers – all delivered by the same group of staff.

5.17 We have assessed our current capacity in terms of technology support. We reviewed this against the key tasks and roles suggested by the Government in terms of technology support to determine the changes we need to make to current staffing roles and the additional resources required to deliver on an ambitious programme of change, while at the same time providing a safe and secure technical environment. This takes account of the tasks outlined previously in this paper and the changes to our technology environment we need to make as part of our security and resilience strategy.

5.18 We have also undertaken a benchmarking exercise with other Councils to assess their capacity and structure. At the moment our costs including support costs appear to be lower than nearly all Councils including much smaller Councils. This has an impact on our ability to deliver on our transformation aspirations, maintain the infrastructure we have, support services to review their provision and importantly to ensure our network and systems are as secure as they must be. This latter point is critical in going forward. While we aspire to be flexible and agile, this increases the risk to the Council. We need to increase our security capacity to manage that risk while ensuring we deliver on service imperatives.

5.19 Part of our review of roles has been to determine the resource we have to support the security of our network, systems and data. At the moment this role is carried out by officers who have other significant tasks. It is important going forward that we separate the role of ensuring the security of our networks, systems etc. from the development and maintenance of our technology.

5.20 To support more agility in our use of technology whilst recognising the increasing risk to services as we move to digital first, we have revised our Information security policy (ISP)and acceptable use policy (AUP). These amendments are intended to be more permissive in approach i.e. recognising that employees and Members will use equipment provided by the Council for a number of purposes i.e. for work but also for personal tasks. We have therefore changed the information security policy and underpinning acceptable use policy to ensure our employees and elected members are given clear guidance on these matters whilst recognising the need for security.

5.21 There is always a balance to be struck in developing such policies. We have sought out best practice in other organisations to develop these. We have also taken account of guidance in terms of GDPR and also cyber security regimes that govern our systems and network. Some of these run against out aim of being permissive and thus we have to find a balance that works for the Council. Both the ISP and the AUP have been to the Corporate Partnership Forum.

5.22 Approval is now sought for both these polices. We are currently determining how we will ensure these are signed off by employees and Members. It is proposed that we would seek to incorporate these into on line training that is required each year but this will be confirmed in due course.

5.23 We will therefore determine the resources we need to support our IT estate and determine how best to meet the gaps. This will include engaging with our Councils to jointly share resources, looking to reduce costs in other areas e.g. network spend etc. Our priority in this work will be to establish an IT security team that would over see our cyber resilience, network security and work with services to support them to work with suppliers to realise ambitions in a safe and secure way.

5.24 We will seek to retrain and refocus our existing staff to make sure we are maximising our current resources and have engaged in early discussions with the Local Government Digital Office on this work. This includes significantly changing the way we support services through our service desk so that we can support people working differently across the Council.

6. Implications

Financial

6.1 The cost of delivering changes in the way the Council delivers services means putting additional resources into those areas that will support that change. Additional resources to take forward our approach to service redesign have been allocated through the change fund by the Council of the Future Board. We have also funding for additional web developers and a quality assurance role. This totals circa £200k for a year. The Board recognised that this funding however would have to be considered going forward as our service delivery changes and this becomes business as usual. In addition, significant money has been allocated through the capital programme including £4.3m to support the implementation of office365, as well as investment to allow us to increase the WIFI capacity, review our network and make sure our infrastructure continues to be safe and secure.

Resources

6.2 The way we support services to deliver change will mean a refocus of our existing support services. In addition we will look at making sure we are utilising all our resources such as software platforms appropriately and to get best value.

Legal

6.3 Nil

Risk

6.4 There is a risk that if the Council does not look to deliver services differently that we will not meet the needs of our customers, not be able to achieve efficiencies and also not provide services that are sustainable in the future. There is a significant risk that the Council can't deliver key priorities and outcomes if we don't change the way we deliver our services or maintain our network capacity and security. This includes delivering on curriculum for excellence etc.

Equalities

6.5 The digital strategy is predicated on making sure we meet the needs of the most vulnerable in our communities. This means promoting digital inclusion but also providing other ways people who are digitally excluded or poor can access quality services. We are underpinning our approach by continuing to invest in digital inclusion projects such as providing WIFI in residential care homes, in the gypsy traveller's site. We will continue to make sure that our approach to digital first does not further exclude people with protected characteristics.

Sustainability/Environmental Impact

6.6 None.

7. Conclusions

7.1 The digital strategy sets out how we can take the next steps in to transform the services we deliver. It provides a starting point by which we can develop our approach pragmatically but with clear direction. However we have to balance our ambition with the resources we have to not only deliver new projects but just keep what we have working.

7.2 We do need to make sure that we maintain the infrastructure this transformation will rely on. We have identified the resources we need to ensure we have a safe, secure and resilient infrastructure. This will be supported by significant change in the way we deliver support to the Council and our services recognising the changing demands from services, customers and communities.

____

Director of Corporate & Housing Services

Author – Fiona Campbell, Head of PTI, 01324 506004, fiona.campbell@falkirk.gov.uk
Date: 12 April 2019

Appendices

Appendix 1 –Strategy
Appendix 2 – Service Design
Appendix 3 – Update on Technology Strategy
Appendix 4 – Information Security Policy
Appendix 5 – Acceptable Use of ICT Resources

List of Background Papers:

The following papers were relied on in the preparation of this report in terms of the Local Government (Scotland) Act 1973:

- None

Appendix 1

Delivering Modern and Digital Services

1. Introduction

1.1. This paper sets out the Council's digital strategy. This sets out:

- the purpose of a digital strategy
- the principles that will be used to guide our journey to becoming a digital council and why these are important going forward.
- some of the challenges we face and then
- the key actions the council, our leaders and services must deliver if we are to reap the benefits of digital transformation.
- The work that will be put in place to support that transformation and thus the delivery of the strategy – on the condition that the strategy is appropriately resourced.

2. Falkirk's Digital Strategy

2.1. One of the organisation's core purposes is to deliver public services that meet the needs of our communities – now and in the future. In order to make sure that we are actually meeting the needs of our customers with services they value and at a cost we can afford we need to embrace change and transformation. This transformation is at the heart of this digital strategy. As such this digital strategy is essentially a customer strategy, enabled by technology and supported by a range of complementary skills, including IT, business analysis, data analytics, marketing and digital communications.

2.2. This purpose and challenge needs to be at the heart of our organisation as it goes forward. Digital is a critical enabler for any transformation agenda and the benefits to our customers and the Council itself are significant. Our customers are clear that they want increased options to transact online. As far back as the 2010 there were clear messages from the public about making savings by services being delivered online with a reduction in the number of buildings people have to visit. This has the potential to reduce property overheads but also has the advantage of moving to more colocation of complementary services.

2.3. The Council's approach to reform and transformation is set out in our Corporate Plan. This digital strategy sets out in more detail the approach we will take to delivering on those commitments. In particular, it articulates our commitment to delivering services that our customers value and that are efficient and effective. To achieve this, we will commit to transformation that focusses on customers´ needs, expectations and experiences through the consistent application of a design process and framework.

2.4. The digital strategy we are pursuing has three key elements:

- Leadership
- Services redesigned to maximise use of digital, improve customer services and reduce costs
- Rock solid technology

2.5. These three elements mirror the digital strategy for local government published last year by the Local Government Digital Office. All Council services need to focus on how they can use technology at all levels to improve services, communicate, engage with citizens more effectively and reduce costs. To achieve this, leadership from senior officers and elected members is required, alongside solid technology platforms that our citizens and our employees will trust and use.

2.6. By delivering on digital the following outcomes will be achieved:

- Citizens will choose to use digital to find information, engage with the Council, access services and self-serve – and they will trust it
- Services will be transformed to include digital delivery based on data analytics and new services will be digital first and by design
- Savings will be realised through more efficient processes, channel shift and a reduction in legacy systems
- Increasingly, internal transactions will become digital

2.7. The key benefits to the Council and our communities are:

- Services will be more efficient, responsive and standardised
- Overly bureaucratic processes that underpin services will be reviewed and streamlined
- Decisions on service delivery will be based on sound evidence from our customers
- There will be more flexibility to customers and communities in the way they engage with the Council
- Our workforce will be more mobile, flexible and able to serve our customers timeously in their communities and therefore less reliant on physical buildings
- Improving access to our data about our services will empower our communities.

2.8. Our strategy will reflect the national strategy in that it is agile, flexible and able to respond quickly to changing circumstances and needs. We therefore will not be preparing a normal paper-based action plan but will, through the delivery of projects that underpin each of the three priorities, look to support the Council in achieving the transformation and efficiencies it requires.

2.9. Our approach will be supported by and informed by our work with the Local Government Digital Office. The LGDO supports local government in its digital transformation journey – working with 31 Councils to support them to deliver better services in the best way possible by sharing resources and skills.

2.10. To date, work on digital service delivery within the Council has been taken forward using existing resources supported by training, upskilling or employing temporary staff, however we know the Council's continued move to digital service delivery, covering online transactional services, communication, engagement, etc. will become the new norm. We need to determine the resources and the skills that are required to support this fundamental transformation. Elected members and Services have become more engaged in current activity and energised about potential future developments. In additional, digital has emerged as a strong theme in the Council of the Future engagement sessions, to the extent that it is identified as one of four key priorities. This is to be welcomed; however this needs to be tempered by recognition that the resources to deliver on expectations are limited and what can be achieved will be directly related to available resources.

2.11. It must be stressed that our move towards a digital council is not just about service delivery but about how we engage with all our communities. As we reduce our physical presence in communities, we need to find different ways to engage with citizens not only to deliver services to them but also to address issues that are important to them and their communities. Our move to a Digital Council must recognise this change in engagement and communications. This is supported by the introduction of the Advice hubs and outreach service that provides targeted face to face support for who need our help most whilst promoting self service to those who have the means and ability to self serve.

Leadership

2.12. In terms of digital leadership, this means having clarity about the services we provide and how they will be delivered in the future to meet the needs of our customers and making sure transformational projects are being put in place to deliver that change. It means ensuring that employees are digitally skilled to use appropriate technology to deliver services in response to customer need, but also to take advantage of the opportunities technology gives us to understand what those needs are through data analysis, behaviour tracking and digital engagement.

2.13. Digital leadership means

- The Council will embrace the digital strategy and realise its benefits
- Our people i.e. citizens, employees and leaders will have the skills and culture to embrace digital
- Our Council will have the capacity and capacity to deliver digital transformation
- Our Council will have capacity for research and development

2.14. Leaders within the organisation must understand the new norm and make sure they have the vision to transform their services. Leaders must understand that digital is not about moving existing services online but a total redesign of services based on the needs of citizens and supported by digital capabilities.

2.15. The Council participated in an independent digital maturity self assessment last year. This was facilitated by the Local Government Digital Office and involved all Directors, Heads of Service and Managers within the Council. This highlighted a number of issues that need to be addressed including:

- Lack of knowledge and the art of the possible
- Assumption that digital is solely an issue for ICT
- Acknowledgement of the potential to use technology to deliver better services
- No clarity about who is responsible for digital transformation
- Need for reverse mentoring – senior managers not comfortable with technology or its potential
- Our customers are using technology to gather information and transact online – we are a step behind where our customers need and expect us to be
- Lack of resources to deliver on our ambitions
- Lack of skills and investment; and
- Critically, the lack of coherent and challenging governance

2.16. A summary of the outputs of the digital maturity self assessment are attached at Appendix 1. The summary findings are being used in two ways

- To inform the contents of this strategy
- To provide a benchmark by which to measure progress over the time of this strategy.

2.17. The assessment carried out by the LGDO showed that digital transformation is not uniformly understood across the Council. Work needs to be done to articulate this vision and ensure a clear understanding of digital principles is full embedded across the organisation, particularly at manager level.

Transforming Services by Design

2.18. The services we deliver need to be designed around the citizen - their needs and expectations. To do this we must radically rethink what we deliver and the way we deliver those services. Currently the majority of our services are delivered on a traditional model that is based on face-to-face engagement focussed on buildings. This neither meets the changing demands of many of our citizens, nor is it affordable. Where we do seek to improve what we deliver, we often approach this improvement from the perspective of the organisation, rather than the needs and expectations of the people who want to use our services. In addition, service redesign is not undertaken across the organisation in accordance with a set of consistent principles, leading to a fragmented and confusing experience for our service users.

2.19. Our Corporate Plan sets out clearly the expectation that we will change and reform what we deliver to be customer-focussed, efficient and effective. This means looking at services from the perspective of the customer – across organisational boundaries and historical structures – clearly defining what the problems are and simplifying our customer journeys. We want to provide a consistent experience for the customer, whether they are interacting with us online, via the contact centre or in person at one of the Hubs. This means we must challenge existing practices if we are to truly transform our delivery.

2.20. We must:

- Set and define standards of good service design and apply them to a whole service approach i.e. look at services from the customers perspective – not by span of management.
- Help services build a new norm that will make services easier to join up – a new shared digital infrastructure
- Make sure we develop the people and skills to make this happen

2.21. The definition of a service is something people use but do not own. Service design is the act of shaping those services and experiences so that they work for the people that use them. It is about bringing design and disruptive techniques to an organisation to reimagine services from a customer perspective.

2.22. This approach to service redesign is critical to digital transformation. We cannot digitally transform services without fundamental redesign. This means thinking differently and delivering differently, an approach which has underpinned our approach to the redesign of advice services, resulting in the Hub model. In this redesign we sought to understand firstly who uses our services, why they used them and then clarified if those people were actually our core customers. This analysis helped us understand that the people using our existing services were not those who needed most support. This understanding led to further engagement with those who potentially needed support but were not accessing it, with a redesign based on their needs. This redesign was developed in parallel with the provision of alternative channels for those who would be displaced in this redesign.

2.23. This example demonstrates transformation does not necessarily mean providing services online. It does mean changing services based on customer needs and using technology to support that change.

2.24. Taking this into account, our current approach to changing services is not deep enough. Some of our processes are historic, with work arounds built on top of work arounds. Redesign needs to start with users, not digitising existing processes that have on the whole been developed to suit the organisation.

2.25. Considerable work has already been undertaken as part of the technology strategy to build a foundation that will support digital transformation of services.

2.26. A critical part of this was the complete redevelopment of the Council's website. The website is the front-end platform for the delivery of online services to our customers and is subject to constant revision and redevelopment to improve the customer journey. This has been recognised by SOCITM which awarded the site the maximum four stars in its 2018 review, one of only five Councils in Scotland and 38 in the UK to achieve this.

2.27. In December 2016 we launched My Falkirk. This is our citizens' account, delivered through the national My Account platform and supported by the Firmstep application. As well as being used directly by citizens themselves, the system is being used by customer services advisors in frontline offices and by the contact centre so is effectively an integrated CRM solution for the Council. Around 40 transactions are now available via My Falkirk and all of these are directly integrated to the back office.

2.28. To date, nearly 25,000 My Falkirk accounts have been created by customers and over 118,000 online transactions have been carried out via the system. Based on SOCITM's model transaction costs of £8.62 for face-to-face, £2.83 by phone and 15p for online, the cost of these transactions would have been £1,142,115, £335,986 by phone and reduced to £17,808 online. While this is just an illustration based on generic costs, it clearly demonstrates the benefits to the Council of being able to deliver more fully-integrated services online.

2.29. Increasing the number of services offered via My Falkirk is dependent on a number of factors including:

- The benefits of each project to customers
- The resources assigned to service design, web enablement and process review tasks; and
- The resources Services put into user acceptance testing and sign off.

2.30. Key to the success of My Falkirk is the consistent approach to service design. To date, we have found that many internal processes require thorough review to ensure that the customer journey is as clear and intuitive as possible, informed by customer need and underpinned by agreed principles for service design.

2.31. The Director of Design and Service Standards for the UK Government has recently published a template of principles and these are attached at Appendix 2. It is recommended that the Council adopts these principles and uses them consistently to redesign our approach to service delivery.

2.32. Dundee City Council is leading on this work strand for the Local Government Digital Office and learning from their approach will inform how we take this forward.

2.33. To support this we will look to adopt a clear framework for ensuring our approach to transformation is consistent with these principles and underpinned by robust technology. This will be through the development of the Scottish Government's Digital First Service Standards. This gives us a core set of questions to assess our approach to technology and indeed use of resources. It allows projects to be assessed against 22 criteria that include issues such as user research, content design, product assessment, technical specification, sustainability security etc. One of product of this digital strategy will be clarity about what the Councils expectations are with regards digital transformation with this framework supporting services in that transition.

Rock Solid Technology

2.34. How we deliver our services is changing significantly. To support this underpinning technology must be reframed to be agile, flexible, secure and robust. We will have people accessing services in very different ways and our infrastructure must allow for this change and progression. We used to rely on buildings to deliver services, now we rely on technology. This means investment in infrastructure and support. Our technology must give firm and secure foundations for future service delivery.

2.35. Our infrastructure has served us well for years and has undergone significant changes to allow us to move to the next phase of transformation and change. This means moving away from rigid systems and networks to connected, consistent, agile and secure approach. This will also mean using industry and sector norms rather than bespoke solutions, we will also be more proactive in ensuring consistency in delivery and approach across the organisation.

2.36. Over the last number of years we have put in place the foundations for change. Some of these significant developments are set out in Appendix 3.

2.37. Over the coming years we will have an even greater reliance on technology to support the delivery of services and in some instances to deliver services. This may include:

- using the internet of things i.e. network of physical devices, vehicles, home appliances and other connected items, to deliver more intelligent solutions and providing data to allow us to monitor more actively services
- artificial intelligence solutions potentially undertaking some of our repetitive processes
- delivering education, tele heath and tele care in very different ways
- supporting a virtual and mobile workforce to connect with citizens, communities and colleagues

2.38. We need to also use technology to engage more with our communities not just in service delivery but in understanding the things that matter to them and the decisions that affect their lives. This means being more creative about our use of technology while at the same time making sure our systems and data is secure.

2.39. Our use of technology has to be planned. We need to make sure that we are applying a rigorous framework to all our digital projects. To this end we will be looking to develop the Scottish Government’s Digital Service Standards in conjunction with services to ensure we have a robust framework for assessing our changes in our technology environment. These standards will seek to assess projects against criteria such as:

- Understanding of user needs in line with design principles
- Simplicity and usability
- Channel shift – move to on line
- Consistent user experience – consistency across applications and throughout a transaction – however that transaction takes place
- Data driven – using evidence from citizens and transactions to drive change and improvement
- Sustainability and continuously improving
- Technology appraisal including security, PEN testing etc.
- Information governance – making sure our systems have robust standards of governance
- Green ICT – reducing our carbon footprint, reusing technology etc.
- Data hosting and data centres – minising cost of hosting systems etc while maximising security and resilience
- Performance management – making sure our systems are producing information that is being used to monitor and review what we are delivering, to whom, at what cost and for what effect.
- Operational acceptance - Are we making sure users are involved in working the system in the way intended.

2.40. This assessment framework will be developed over the coming months to ensure that our technology solutions are fit for purpose not just now but in the future.

3. What Do We Need To Do To Become A Digital Council?

How do we change and transform

3.1. To understand where we are on the journey to delivering digital services, a self assessment was undertaken in partnership with the Local Government Digital Office to asses our digital maturity. This outlined the following challenges for the Council:

- Understanding what digital is and how we manage change.
- Ensuring our governance arrangements are fit for purpose and deliver on this strategy in a way that drives change
- how we manage demands on limited resources needs to be strengthened
- Ensuring a consistent approach to our systems and network if we are to provide joined up services.
- Balancing on-going maintenance and development
- Articulating the vision through a clear strategy.
- Applying principles of service design consistently, robust and with energy
- Capacity for digital transformation needs to be increased.
- Our main delivery through our policy, technology and improvement teams needs to be strengthened and made more resilient.
- The capacity of our support to make sure technology is safe, secure and working needs to be increased
- The skills of our staff need to be developed.
- The skills of our communities to use the technology needs improved.
- Investment in the right technology.
- Need to have capacity for research and innovation
- Change and forward thinking is critical to ensure we are delivering services in a way our customers expect and need. We therefore need capacity in this key area.
- Our change and transformation needs to start with the citizen. We will therefore support services through the application of service redesign principles to re think what services we deliver and how we deliver them.

3.2. To address these challenges we need to do things differently and we need to resource change.

Leading a Digital Council.

3.3. To become a digital council we must have leaders that support digital first and by design. Our leaders, service managers and politicians will:

- Make sure that digital expertise is central to our decision-making and that all technology decisions are approved by the appropriate person or committee. This will ensure that we are using our collective purchasing power to stimulate a speedy move towards change.
- Have visible, accessible leaders throughout the organisation who support those who champion this strategy to try new things and work in and amongst colleagues.

- Support our workforce to share ideas and engage in communities of practice by providing the space and time for this to happen.
- Try new things, from new digital tools to experiments in collaboration with other organisations.
- Champion the continuous improvement of cyber security practice to support the security, resilience and integrity of our digital services and systems.

Delivering a Digital Council

3.4. To support the delivery of a digital council our improvement, information, technology and digital teams will make sure that we support the Council and services to:

- Research how to reuse existing user research, service design, common components, and data and technology standards before starting to design or procure something new. This will be through the application of the Scottish Government's digital design principles.
- Build capacity in service design, so that each service we transform is quality controlled against our national service standard where appropriate.
- Ensure every new technology solution procured must operate according to the technology code of practice, putting us in control of our service data, using open standards where they exist and contributing to their creation where they don't.
- Share knowledge about digital projects particularly where there is an opportunity for potential reuse or collaboration with others.
- Work together to establish the trust frameworks we need to safely analyse and share personal data. This will allow us to better serve our shared customers and reduce the need to ask citizens for the same information multiple times.
- Work together to create common solutions that allow us to check people's eligibility for services in real time with their consent.
- Take inspiration and ideas from a wide range of sources, and participate individually in communities of practice and interest outside the organisation (for example, the Local Government Digital Office, and related networks and events).
- Make sure we have the right skills to deliver and benefit from digital services – from those that support this ambition to those that use our services.

Supporting a Digital Council

3.5. To ensure we are supporting our digital ambitions with an appropriate rock solid technology we will:

- Establish an IT network and security group to ensure we comply required external accreditation and the Scottish Government Public Sector Cyber Resilience plan to keep our people and information safe and secure.
- Seek to provide appropriate training and support to services to increase the pace of delivery of new technology and ensure that staff has the necessary training and support to use the new technology effectively.

- Create drop in points so that technology can be issued or replaced when faulty quickly.
- Expand our customer support so that it is available out with usual office hours and that our support better reflects the needs of a changing mobile and flexible work force.
- Ensure we utilise our technology estate effectively, efficiently and consistently across the Council
- Restructure the existing IT resources and support to allow us to concentrate on the delivery of projects
- Plan our ICT infrastructure better with the introduction of a Enterprise Architect role
- Deliver a business case for Office365 that allows us to move to support a more mobile workforce with the tools they need to collaborate and be productive.
- Develop a strategy to increase the resilience of our technology through a move to externally hosted cloud based solutions
- Support our services to deliver for their customers
- Ensure we have a sound approach to research and development.

Appendix 2

Services are what you use, but do not own.

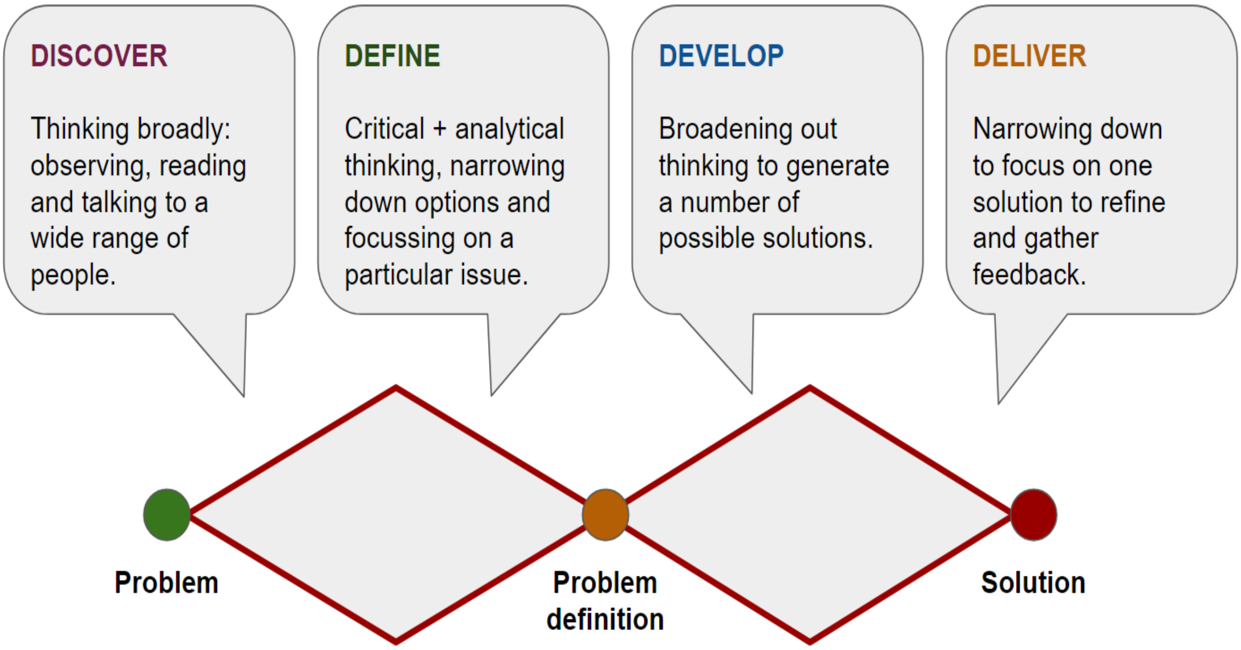
Service design is the act of shaping those services and experiences so that they work for the people that use them.

Double diamond design process

Divided into four distinct phases – Discover, Define, Develop and Deliver – the Double Diamond is a simple visual map of the design process.

In all creative processes a number of possible ideas are created ('divergent thinking') before refining and narrowing down to the best idea ('convergent thinking'), and this can be represented by a diamond shape. But the Double Diamond indicates that this happens twice – once to confirm the problem definition and once to create the solution.

One of the greatest mistakes is to omit the left-hand diamond and end up solving the wrong problem.


DISCOVER
Thinking broadly: observing, reading and talking to a wide range of people.
DEFINE
Critical + analytical thinking, narrowing down options and focussing on a particular issue.
DEVELOP
Broadening out thinking to generate a number of possible solutions.
DELIVER
Narrowing down to focus on one solution to refine and gather feedback.
Problem
Problem definition
Solution

15 principles of good service design

A good service must:

1. Enable a user to complete the outcome they set out to do

A good service enables a user to do the thing that they set out to do from start to finish – be that start a business or learn to drive – in as much of a seamless stream of events as possible. This includes the moment that a user is considering a task to the moment they have completed it – and any necessary steps or support, change or amendment thereafter.

2. Be easy to find

The service must be able to be found by a user with no prior knowledge of the task they set out to do. For example someone who wants to 'learn to drive' must be able to find their way to 'get a driving licence' as part of that service unaided.

3. Clearly explain its purpose

The purpose of the service must be clear to users at the start of using the service. That means a user with no prior knowledge must understand what the service will do for them and how it will work.

4. Set the expectations a user has of it

The service must clearly explain what is needed from the user in order to complete the service and what they can expect from the service provider in return. This includes things like how long something will take to complete, how much it will cost, or if there are restrictions on the types of people who can use the service.

5. Be agnostic of organisational structures

The service must work in a way that does not unnecessarily expose a user to the internal structures of the organisation providing the service if those structures run contrary to the task a user is trying to achieve.

6. Require the minimum possible steps to complete

A good service requires as minimal interaction from a user as possible to complete the outcome that they're trying to achieve. Sometimes this will mean proactively meeting a user's needs without them instigating an interaction with your organisation. This may occasionally mean slowing the progress of a service in order to help a user absorb information or make an important decision.

7. Be consistent throughout

The service should look and feel like one service throughout – regardless of the channel it is delivered through. The language used should be consistent as should visual styles and interaction patterns.

8. Have no dead ends

Regardless of whether or not a user is eligible for suitable for a service, the service should direct all users to a clear outcome. No user should be left behind, or stranded within a service without knowing how to continue, or being provided an easy route to do so.

9. Be usable by everyone, equally

The service must be usable by everyone who needs to use it, regardless of their circumstance or abilities. No user should be adversely unable to use the service more than any other.

10. Respond to change quickly

The service should respond quickly and adaptively to a change in a user's circumstance and make this change consistently throughout the service. For example, if a user changes their phone number online, their phone number should be recognised in a face to face service.

11. Work in a way that is familiar

People base their understanding of the world on previous experiences. If there’s an established custom for your service that benefits a user, your service should confirm to that custom. For example, users who have signed up to a new service often expect an email confirmation acknowledging their sign up. Avoid customs that negatively affect your user (such as pre-selecting a ‘send me marketing emails’ tick-box) or following customs that are inefficient or outdated.

12. Encourage the right behaviours from users and staff

The service should encourage safe, productive behaviours from users and staff that are mutually beneficial. For users, the service should not set a precedent for behaviours that may put the user at harm in other circumstances – for example, providing data without knowing the use of that data. For Staff, this means they should not be incentivised to provide a bad service to users, for example through short call handling time targets.

13. Clearly explain why a decision has been made

When a decision is made within a service, it should be obvious to a user why this decision has been made and clearly communicated to the user at the point the decision has been made. A user should also be given a route to contest this decision if they need to.

14. Make it easy to get human assistance

A service should always provide an easy route for users to speak to a human about an issue if they need to.

15. Require no prior knowledge to use

A service should not use language that assumed any prior knowledge of the service from the user.

Appendix 3

1. Update on Technology Strategy

1.1. Since approving the Councils technology strategy in 2014, we have been progressing 3 priorities of:

- Customer access
- Flexible and collaborative working
- Well managed information

Telephony

1.2. The Council recently started the significant step of replacing all its telephony – from mobile and desk based phones to the call management system that supports front line service delivery. This change will ensure customer calls made to the Council's telephone number will be handled in a different way, ensuring that all calls will be directed appropriately.

1.3. Combining the new telephony system with the flexibility of mobile working will also allow employees to receive calls wherever there are based, tying in with agile working and again maximising service accessibility for customers. By unifying our communications, the telephony system will provide further functionality including

- video conferencing;
- the ability to link telephony with calendars showing staff availability
- instant messaging - allowing for collaboration opportunities between staff and reducing the need for email.

1.4. All of which increases flexibility for employees and our customers alike.

Flexible and Collaborative Working

1.5. In December 2014, the Council took the decision to make a substantial investment in mobile and flexible technology. Undertaking this ambitious project meant the Council would be able to deliver services to our customers in an agile way away from fixed desks and buildings, taking services directly to where they are most needed. To achieve this major change, significant challenges had to be overcome. Information had to be managed in a secure way, minimising risks to our customers by ensuring their data is handled appropriately. This meant many of the applications in use by services needed to be changed to work through a central, secure system and supported by the technology which would allow that to happen. The technology the Council invested in to achieve this is provided by a world leading security organisation (Citrix) and is used by many public and private organisations across the world. This technology change means that most officers can access their desktops remotely and thus the systems they use daily over a secure network. The approach provides a different approach to the way we are able to deliver our services by putting our customers' need to the forefront of service delivery. It provides the Council with greater flexibility in the way we manage and use our property assets. By enabling a review of our property portfolio, we can significantly in contribute to the financial savings the Council requires to achieve.

1.6. Additionally our investment in mobile and flexible working technology has minimised the need to replace or upgrade desk top computers. As a result the Councils PC replacement programme has ended providing a significant annual saving to the Council.

Replacement of Social Work System

1.7. One of the Council's more important systems – our Social Work Information System - will be replaced this year. This change will significantly improve the service that can be provided to our most vulnerable citizens by providing real time information to workers. This new system will also allow us to share information securely and appropriately with partners to support better collaboration and thus outcomes. The system provides the opportunity to bring information together in a way which was never previously available. Families and acquaintances can be easily linked together providing an overall picture of a social work case, offering increased risk management and valuable information for officers and our partners. It is anticipated, after implementation and training, the go-live period will be the second quarter of 2019.

Wi-Fi

1.8. We are undertaking a programme of providing a more flexible network for our staff so that they will be able to connect to our network from any building. This will also be used to allow the public to access Wi-Fi and thus connect to Council and other services from our buildings.

Security

1.9. A principled approach to digital services must be founded in providing a secure and trusted environment. To facilitate this, the Council has invested significant effort in developing a robust patching and upgrading regime and supports our business. As we become ever dependant on technology as the foundation of our service delivery, then we must be more diligent in our approach to security. This must not be at the expense of agile, flexible and joined up services.

1.10. The Scottish Government Public Sector Cyber Resilience Action Plan rightly places ever more burdens on the council in managing the ever present risk.

Appendix 4

INFORMATION SECURITY POLICY

1. Definition of Information Security

Information security is the protection of information (in any form including hand-written, typed, video, paper based or electronic) from a wide variety of threats. The purpose of this is to minimise business risk, ensure business continuity, support information sharing, achieve organisational objectives, develop business opportunities and protect information relating to people.

2. Aim of the Policy

The purpose of this policy is to ensure:

- **Confidentiality of information:** making sure that information is accessible only to those authorised to have access.
- **Integrity of information:** safeguarding the accuracy and completeness of information and data processing methods.
- **Availability of information:** making sure that authorised users have access to information and assets when required.
- **Protection of people:** making sure personal information is safe.
- **Regulatory compliance:** making sure that the Council meets its regulatory and legislative obligations. See Appendices 1 and 2.

3. Policy Scope

This policy concerns information in all forms printed, handwritten or verbal; stored on paper or stored electronically; transmitted by post, fax or transmitted electronically, carried on paper or on PCs, laptops, tablets, smartphones, blackberries, or USB devices.

This policy applies to all employees and elected members whether working in Council premises, working at home, or when mobile working. It also applies to employees of external organisations who use, or access, the Council's Information and Communications Technology (**ICT**).

4. Policy Statement

Information security is an essential enabler in helping the Council meet its objectives. Security risks must be managed effectively, collectively and proportionately to achieve a secure and assured working environment. The Council's processes and procedures must reflect the principles, governance and responsibilities set out below.

5. Principles

Data must have an appropriate level of protection applied at all times.

5.1 Much of the information handled by the Council relates directly to individuals and it is important their information is protected from loss or theft either accidentally or deliberately.

A risk based approach must be adopted.

5.2 It is important that controls are applied in a proportionate way so that information is protected in a way which does not hamper business process and costs/benefits are optimised.

Information security must be a priority in all partnerships.

5.3 Good security is crucial to building trust with partners and those with whom we share information. All data sharing initiatives should consider security at the outset and, where personal data is involved, take a *data protection by privacy and design* approach. This will include the use of data protection impact assessments at the outset of initiatives where there is a high risk to the privacy of individuals. All data sharing will be governed by formal written agreements.

Ownership, and access to information and rights to it, must be clearly defined, controlled and reviewed through formal processes.

5.4 Owners of information must carry out regular reviews of user access rights and in particular must withdraw rights promptly when staff leave or change roles. A hierarchy of information ownership should be created in the event that information owners leave or change roles so that continuity of information ownership is maintained.

Plan for the unexpected.

5.5 Regardless of vigilance, vulnerabilities will be found, new attacks will take place and the surprising will happen. Processes must be flexible enough to cope with the unexpected. Security defences must be layered so as to provide cover should one layer fail and risks from single points of failure must be managed. Business continuity plans must be prepared and tested where appropriate.

Security by design for the whole lifecycle.

5.6 Security should be built in from the start, not bolted on later, to avoid expensive redesign or vulnerabilities. All initiatives must consider security at the outset and, where personal data is involved, take a *data protection by privacy and design* approach, including the use of data protection impact assessments at the outset where there is a high risk to the privacy of individuals. During the operational life of an asset, processes and procedures should be maintained, resources monitored, future capacity needs planned for and changes strictly controlled. At the end of an asset's life it should be disposed of carefully as insecure disposal can expose confidential information.

All employees and elected members are accountable for their actions.

5.7 Information security responsibilities must be clearly defined and communicated. Training provision should be in accordance with corporate arrangements. All user access accounts must be identifiable with an individual. Segregation of duties is an important information security control mechanism that should be used where appropriate. Individuals must act in accordance with this policy, and the other policies listed in Appendix 3. Failure to do so may result in disciplinary action. All breaches of these policies will be fully investigated.

6. Governance and Responsibilities

In order to ensure security of information, the following governance arrangements are required within the Council to make sure the organisation meets its business aims and objectives.

6.1 **The Corporate Management Team (CMT)** recognises the importance of information security to the organisation and directs the Council's strategy, setting the overall direction and making sure resources for implementation.

6.2 The Director of Corporate and Housing Services is the Council's **Senior Information Risk Owner (SIRO)** and has lead responsibility to ensure that organisational information risk is properly identified and managed in the Council and that appropriate assurance mechanisms exist. The Council's Financial Regulations provide that the Director of Corporate and Housing Services is responsible for the issue of this policy. Also, in terms of the Financial Regulations, the Director, in consultation with the Chief Governance Officer, is responsible for ensuring that proper privacy and security is maintained in respect of information held on manual or computer records, and that the requirements of relevant legislation are complied with.

6.3 **The Information Management Working Group (IMWG)** is chaired by the Chief Governance Officer and seeks to (i) promote the effective management of all Council information in all formats throughout its lifecycle, to meet operational, legal and evidential requirements, (ii) support the Council in identifying and managing its information needs, risks and responsibilities, and (iii) ensure an information risk management policy and framework is in place and overseen.

6.4 **The IT Security Group** is chaired by the Head of Policy Technology and Improvement and has the following responsibilities - (i) in conjunction with the IMWG, the promotion of Information Security throughout the Council, (ii) the review and recommendation for the approval of all IT-security related policies and procedures, (iii) compliance and certification through external assurance schemes such as PSN and Cyber Essentials, (iv) review and monitoring of IT security incidents, their cause, resolution and future prevention, and (v) providing technical input to the DPIA assurance process.

6.5 **The Head of Performance, Technology and Improvement** has overall responsibility for the security of the Council's corporate technology systems and network.

6.6 **The Data Protection Officer** is responsible for monitoring the Council's compliance with data protection legislation and with its policies in relation to the protection of personal data.

6.7 **The Corporate Risk Management Group (CRMG)** is chaired by the Head of HR and Business Transformation (who is also a member of CMT). The CRMG receives regular reports on information asset and cyber security risk management and makes sure that appropriate control objectives and key controls are established to address any weaknesses identified.

6.8 **Information Asset Owners (IAOs)** are identified as Directors or Heads of Service at a service area level and will be accountable for ensuring that the risks in relation to the assets are identified and managed according to the appropriate level of security. This includes user access management. IAOs must also clearly define data retention and disposal requirements.

6.9 **Internal Audit** will regularly review information security matters through its audit programme. This will serve to inform the risk management approach and promote continuous improvement of policy.

6.10 **All staff and elected members** are responsible for protecting information in accordance with this policy.

7. Information Security Incidents

An information security incident is an event that has, or could have, resulted in loss or damage to information, or an event which is breach of this policy. This includes but is not limited to:

- The loss of an unencrypted memory stick
- Theft or loss of data held in electronic format
- A break-in to Council premises
- Paper files going missing
- Disclosure of confidential information
- Unauthorised access to a system
- Unauthorised use of information
- Cyber attack

Information security incidents must be reported as set out in the Information Security Incident Reporting Procedure.

8. Review of Policy

This policy will be reviewed every 3 years or sooner if required by changes to legislation, technology or Council policy.

The SIRO will be responsible for ensuring the review of this policy.

APPENDIX ONE

Legislation

Information security is managed in accordance with the following legislation.

The Copyright, Designs and Patents Act 1988	UK copyright law which gives creators of literary, dramatic, musical and artistic works the right to control how their material may be used.
The Computer Misuse Act 1990	This was created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The act has been modified by the Police and Justice Act 2006.
Data Protection Legislation as defined by the Data Protection Act 2018	The main piece of legislation that governs protection of personal data in the UK. It provides a way that individuals can enforce the control of information about themselves.
Human Rights Act 1998	This act governs interception or monitoring of communications, especially article 8 which guarantees respect for an individual's private and family life, their home and correspondence. Public authorities can not interfere with these rights unless it's justifiable to do so.
Regulation of Investigatory Powers Act 2000 and Regulation of Investigatory Powers (Scotland) Act 2000	Aims to make sure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.
Electronic Communications Act 2000	Gives legal recognition for electronic signatures and makes it simpler to amend existing legislation that could hamper the development of internet services.

Telecommunications Act 2003	Governs fraudulent and improper use of telecommunications equipment
Freedom Of Information (Scotland) Act 2002	Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner.
The Privacy and Electronic Communication (EC Directive) Regulations 2003	Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover issues relating to privacy of electronic communications including telemarketing and cookies.
Public Records (Scotland) Act 2011	The council must prepare a records management plan setting out arrangements for the management of the authority's public records.

APPENDIX TWO

Standards

Information security is managed in accordance with the following standards.

STANDARD	DEFINITION
Information Technology Infrastructure Library (ITIL)	A set of concepts and techniques for managing information technology, infrastructure, development and operations.
ISO/IEC 27001 and 27002	International standards for information security management.
National Information Assurance (IA) Strategy (2007)	This outlines an approach for the UK in adopting information risk management by making sure the correct level of professionalism, education and training; availability of IA products and services as well as compliance and adoption of standards.

Payment Card Industry Data Security Standards (PCI DSS)	Standard developed by major credit card companies as a guideline to help organisations that process card payments to prevent fraud and other security vulnerabilities and threats.
Public Services Network (PSN) Code of Connection	The PSN is a private wide area network across which secure interactions between connected organisations can occur (previously known as GSX).
Security Policy Framework (SPF)	The SPF describes the principles and approaches that central government have established to protect its assets, whether they be people, infrastructure or information and at the same time assist in the delivery of public services. The SPF applies to all organisations associated with the delivery of public services.
Scottish Government (SG) Cyber Security Action Plan	The action plan, developed in partnership by the SG and the National Cyber Resilience Leaders Board (NCRLB), sets out the action the SG intends to take in order to make progress towards the 3rd outcome of the Cyber Resilience Strategy, "We have confidence in, and trust, our digital public services."
Cyber Essentials Accreditation	Accreditation against a set of basic technical controls to help organisations protect themselves against common online security threats.

APPENDIX THREE

Supporting Documents

To make sure the objectives of this policy are met all staff must comply with the following guidelines. Senior management must ensure the material is understood and adherence appropriately monitored.

- Acceptable Use Policy (including Email Guidelines and Social Media Guidelines)
- Corporate Information Security Guidelines
- Data Protection and Confidentiality Guidelines
- Information Security Incident Reporting Procedure
- Data security breach management procedure
- Mobile flexible working guidance
- Code of Conduct for Employees

Version	Purpose/change	Author	Date
0.1	First draft based on Glasgow	Wendy Barber	28.2.18
0.2	Second draft after discussion with Ian Rennie	Wendy Barber	16.3.18
0.3	With Ian Rennie’s comments	Ian Rennie	
0.4	With Wendy Barber’s comments	Wendy Barber	13.6.18
0.5	At meeting Wendy Barber/Ian Rennie	Wendy Barber	21.6.18
0.6	Final draft	Wendy Barber/Ian Rennie	23.1.19
0.7	Minor change to replace reference to Homeworking Policy to Mobile Flexible Working Guidance	Wendy Barber	2.4.19

Appendix 5

POLICY ON ACCEPTABLE USE OF ICT RESOURCES

1. Introduction

This document sets out our policy and guidelines on the permitted use of our Information and Communications Technology (**ICT**) resources and what action may be taken if you breach this policy. It outlines the minimum standards to be followed by users of our ICT resources. Our ICT resources includes our networks, network equipment, software, applications and IT equipment including telephones.

This policy replaces all previous versions.

2. Users

This policy applies to everyone who uses our ICT resources:

- Council and Falkirk Community Trust staff
- Elected members
- Contractors
- Consultants
- Volunteers
- Interns
- Modern apprentices and graduates
- Any other person who has access to our ICT resources.

This policy does **not** apply to:

- School pupils

3. Responsibilities

All users are required to read this policy and to comply with it at all times.

If you are a manager or supervisor, you must:

- Make sure that your staff are **aware** of this policy and have signed a **user access form** before using any of the ICT resources.
- **Authorise** use of ICT resources for your team.
- Make sure your staff **comply** with this policy when using our ICT resources.
- Deal with **breaches** of this policy (more information in section 8).
- Make sure that if you have **staff changes** – new staff starting, moving or leaving – you complete the relevant forms and send them to HR and ICT. This will allow the access rights to our ICT resources to be correctly updated for the member of staff.

4. Working arrangements

This policy applies at all times, to individuals using our ICT resources whether in our buildings, at home or when mobile working.

This policy applies to:

- PCs and thin-client devices such as I-Gels
- Telephones (including mobile and landlines)
- Mobile devices (including laptops, tablets and iPads)
- USB storage devices
- Business applications (for example MyView, Integra and the social work information system)
- Fax machines
- Our communications network
- Radio systems
- IT connected devices – Internet of Things
- Software
- IT networks

5. Guidelines on personal use of our ICT facilities

You are allowed to use our ICT resources for personal use provided it does not:

- Hinder our business
- Incur any additional cost to use
- Adversely affect the running or our systems
- Bring us into disrepute

Personal use must not:

- breach the general guidelines set out in this policy
- make use of business information which has not been made available to the public (for example our Council Tax system – access is explicitly prohibited and this would be a criminal offence under the Computer Misuse Act 1990 and Data Protection Legislation)

Personal use must not include:

- Allowing others, such as friends or family, to use our ICT resources.
- Using your business email address to subscribe to personal mailing lists and clubs
- Installing and downloading programs or apps not corporately approved
- Using file sharing programs not authorised by the Council
- Using encryption to obscure the content of personal message and files

We will not accept responsibility for:

- Storing backups of personal files
- Restoring copies of personal files from backups on request –
- Any loss you incur as a result of personal transactions made using our ICT resources.

6. General guidance on the acceptable use of our ICT resources

These guidelines apply to both business and personal use.

Software

- Software, including media files such as music and video, must only be used in accordance with licence agreements and UK copyright law. Downloading, making, using or distributing unauthorised software is illegal and is not permitted on our ICT resources.

Personal data

- You must follow our Information Security Guidelines and our Data Protection Guidelines to ensure personal data is kept secure.

Business use of social media

- Staff who use social media for business purposes will be given support and training by their manager in its appropriate use in line with our media protocols.
- If your role requires you to post updates to social media sites, remember you are representing the Council and anything you publish reflects directly on us. If you think you've made a mistake online, notify your manager immediately.
- You should use the same safeguards as you would with any other form of communication. Do not publish personal or other confidential information on social media.
- Always consider any potential risks before publishing on social media and have plans in place to mitigate them.

Personal use of social media

- Guidelines are attached to this policy.

Email and messaging

- Any message you send from our Council email system (or other messaging system) identifies the Council as the sender. Emails, texts and other electronic messages are therefore formal communications from the Council and should be treated as such. You must make sure that any information you send is appropriate and does not include any personal comments that may conflict with our policies or bring us into disrepute.
- You must follow the email guidelines.

Mobile devices

- You must take care with the security of any of our ICT resources, especially mobile devices. Do not leave equipment such as laptops and smart phones unattended in a vehicle or elsewhere.
- You must ensure that all mobiles devices are encrypted.
- You must not store information about citizens, customers or service users on a personal mobile phone or other device.
- If you have cause to contact a colleague's personal mobile phone or home phone but have to leave a message, this should be limited to basic information such as "please call me back". If someone else has left a message on your personal voicemail and this contains sensitive information, you should delete the message once you have listened to it.
- You must exercise caution when using a mobile phone in a public place in order to protect Council and service user information, and yourself.

You must **not** use our ICT resources as follows:

- For illegal activities, including defamation and fraud
- To run personal or private software or apps – there is a risk of viruses/malware to the Council network
- For any purpose that would breach our Information Security Guidelines, our Data Protection Guidelines, our Dignity at Work Policy or our Code of Conduct for Members and Officers.
- To install software or tools which undermine or bypass our security systems and policies. This includes any software that would:
    - Identify passwords for files and accounts
    - Secretly record keyboard input
    - Hide the user's identity
    - Intercept traffic transmitted across the network
    - Provide remote access to the Council's network

The above list of examples is not exhaustive.

If you are not sure whether your use of ICT resources is appropriate, please speak to your line manager.

7. Monitoring of the use of our ICT resources

By using our ICT resources, you accept that your usage may be monitored. Monitoring helps to maintain the efficiency and integrity of our ICT systems. Your use of ICT resources may also be investigated and/or monitored in the event of any investigation into alleged misuse of ICT resources.

8. Breaches of this policy or other misuse of ICT resources

Action will be taken against any individual who breaches this policy, or misuses our ICT resources. The action taken will be appropriate to the circumstances and may include disciplinary action up to, and including, dismissal. We may withdraw your permission for personal use of ICT resources if you have been found to breach this policy.

Breaches of this policy may be reported to the police and/or other professional bodies where appropriate.

If you are aware of any breach of this policy, you should advise your manager or supervisor as soon as possible. Please also refer to the Information Security Incident Reporting Procedure.

9. Employee benefits and resources

We recognise there are benefits to individuals from this policy, which includes the personal use of ICT resources as set out in section 5:

- Responsible and productive use of our ICT resources can enhance your skills and awareness.
- Personal use of ICT resources can help balance your work, lifelong learning and personal life.
- Personal use of ICT resources is an opportunity to provide a benefit to you at no additional cost to us.

You must complete a mandatory information security course each year if you use our ICT resources.   The course reminds you of your responsibilities when using our equipment and how to handle and protect the information you use at work.

10. Other relevant policies

For more information, please read our:

- Information Security Policy
- Information Security Guidelines
- Guidelines on personal use of social media (attached)
- Email guidelines (attached)
- Data Protection and Confidentiality Guidelines
- Information Security Incident Reporting Procedure
- Data Security Incident & Breach Management Procedure
- Code of conduct for employee and members
- Dignity at work policy
- Mobile Flexible Working guidance

Version	Purpose/change	Author	Date
0.1	First draft based on Glasgow	Wendy Barber	28.2.18
0.2	Second draft after discussion with Ian Rennie	Wendy Barber	16.3.18
0.3		Ian Rennie	
0.4	Reviewed at meeting Wendy Barber/Ian Rennie	Wendy Barber	21.6.18
0.5	Updated with changes from FC	Ian Rennie	26.11.18
0.6	Final	Wendy Barber/Ian Rennie	23.1.19
0.7	Minor change to replace reference to Homeworking Policy to Mobile Flexible Working guidance	Wendy Barber	2.4.19
0.8	Format changes	Fiona Campbell	16.4.19