Inverclyde council

AGENDA ITEM NO: 6

Report To:	**Policy & Resources Committee**	**Date:**	**22 September 2015**
Report By:	**Chief Financial Officer**	**Report No:**	**FIN/78/15/AP/LA**
Contact Officer:	**Allan McDonald**	**Contact No:**	**01475 712098**
Subject:	**ICT Services Update and Policy for the Physical Security of ICT Systems**		

1.0 PURPOSE

1.1 The purpose of the report is to update Committee on the performance of ICT Services and to propose a new policy in respect of the Physical Security of ICT Systems.

2.0 SUMMARY

2.1 ICT continues to provide a high level of service despite increasing demand from users and the reduction in resources. It has a range of ongoing projects that will improve reliability and delivery of services and is working with a number of services to identify opportunities to implement new ways of working and drive efficiencies.

2.2 The Servicedesk continues to deliver a high quality service that has rated highly in Customer Satisfaction exercises. There is a challenge to ensure that this is maintained in light of ongoing and increasing resource pressures. The majority of the day to day work that the servicedesk undertakes is in the Schools. With an increasing emphasis on the use technology in the classroom ICT works closely with QIO colleagues in Education Services to ensure that the service delivers in line with educational priorities.

2.3 Digital Access, Channel Shift and Modernisation have called heavily on ICT expertise and services to deliver new ways of working, agile and remote access to services and drive service efficiencies required by Asset and office rationalisation programmes. The success of agile working in HSCP, using EDRMS, Hot Desking and Mobile working has been a key factor in the success of the colocation of HSCP teams in Hector McNeill House. Appendix 2 provides more detail on the relevant projects.

2.4 The Council has a requirement, as part of its PSN Code of Connection Agreement, to ensure the physical security of core ICT Infrastructure. ICT Services has adopted the recommendations within the Cabinet Office CESG Good Practice Guide No 35 – Protecting an ICT Network; however this practice has never been formally adopted as Council policy.

2.5 The policy proposed at Appendix 3 also formalises existing agreements between ICT Services and Legal and Property Services for the security design of Data Hubs in new build and refurbished accommodation.

3.0 RECOMMENDATIONS

3.1 That the Committee note and comment upon the performance detailed in the report and supporting appendices: and

3.2 That the Committee approves the implementation of the new Policy for Physical Security of ICT systems.

Alan Puckrin
Chief Financial Officer

4.0 BACKGROUND

4.1 As part of the ongoing restructure of the Council's Services. ICT Service became part of Finance Services on 1st April 2015.

4.2 ICT Services provides 5 main functions as part of its overall service:

- Servicedesk – Incident Response and Service request
- Server and System Support
- Network and Telecommunications
- Application Support and Development
- Project Management

4.3 The service provides support from 08:40 – 1700 (16:30 Friday) and delivers a highly efficient and very cost effective service. The service is consistently benchmarked as one of the lowest spending services per customer/device of all 32 local authorities.

5.0 PERFORMANCE

5.1 ICT Services provides a range of functions critical to the ongoing delivery of services to staff, pupils and customers of the council. Despite ongoing budgetary pressures, ICT Service has continued to meet and exceed Service level targets. Appendices 1 and 2 show the high level performance across a range of targets:

- Servicedesk Incidents
- Servicedesk Service Requests
- Internet and Web Access
- Email
- PC Refresh
- Projects Update

5.2 Servicedesk Incidents. These tables shows a steady number of incidents being received by the servicedesk on a month by month basis. The number of calls that fail to be resolved within the agreed Service Levels remain low and the overall Service Levels remains well above the current 80% target. An incident is defined as an issue that impacts directly on the ability of a member of staff, a team or department to continue to perform their job. Common examples are PC failures, Application errors, Interactive Whiteboard bulb replacements.

5.3 Servicedesk Service Requests. These tables also shows a steady number of Service Requests being received by the servicedesk on a month by month basis. The number of requests that fail to be resolved within the agreed Service Levels remains low and the overall number remains well above the current 80% target. A Service request is defined as an additional requirement. Common examples are additional network points or equipment, office moves or the provision of a bespoke application.

5.4 Internet and Web Access. This report shows the number of visitors to the main council website www.inverclyde.gov.uk. It shows an improvement in the number of pages being visited since the website was refreshed in May 2015. Ongoing monitoring of this will be highlighted in future reports as more data is collected.

5.5 Email. The Council receives an average of just under 500,000 incoming emails each month. The figures in theses tables show the breakdown of legitimate mail against spam messages and mail that contains viruses and malware.

5.6 PC Refresh Programme. The council currently has a five year PC refresh programme. This table shows the number of devices refreshed in each of the last five years. From 2016/17 a six year refresh programme is being introduced.

6.0 POLICY FOR THE PHYSICAL SECURITY OF ICT SYSTEMS

6.1 The Cabinet Office CESG good Practice Guide No 35 identifies a range of requirement to have suitable physical controls in place to restrict access to core network components.
Finance.

6.2 The policy identifies three different types of location where core infrastructure may be located and details a proportionate set of requirements for each site.

6.3 The policy will become part of the supporting documentation used in the PSN Code of Connection Accreditation process.

7.0 FINANCE

7.1 Financial Implications:

There are no direct costs arising from this report.

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report £000	Virement From	Other Comments
N/A					

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact £000	Virement From (If Applicable)	Other Comments
N/A					

7.2 **Legal**

There are no legal implications arising from this report.

7.3 **Human Resources**

The policy refers to the Council's Data Protection Policy and the Acceptable Use of Information Policy, both of which contain reference to potential disciplinary action in the event of a breach of those policies

7.4 **Equalities**

Has an Equality Impact Assessment been carried out?

x	Yes	See attached appendix
	No	This report does not introduce a new policy, function or strategy or recommend a change to an existing policy, function or strategy. Therefore, no Equality Impact Assessment is required.

Repopulation

7.5 There are no repopulation issues arising from this report.

8.0 CONSULTATIONS

8.1 The proposed Policy has been approved by the Corporate Management Team.

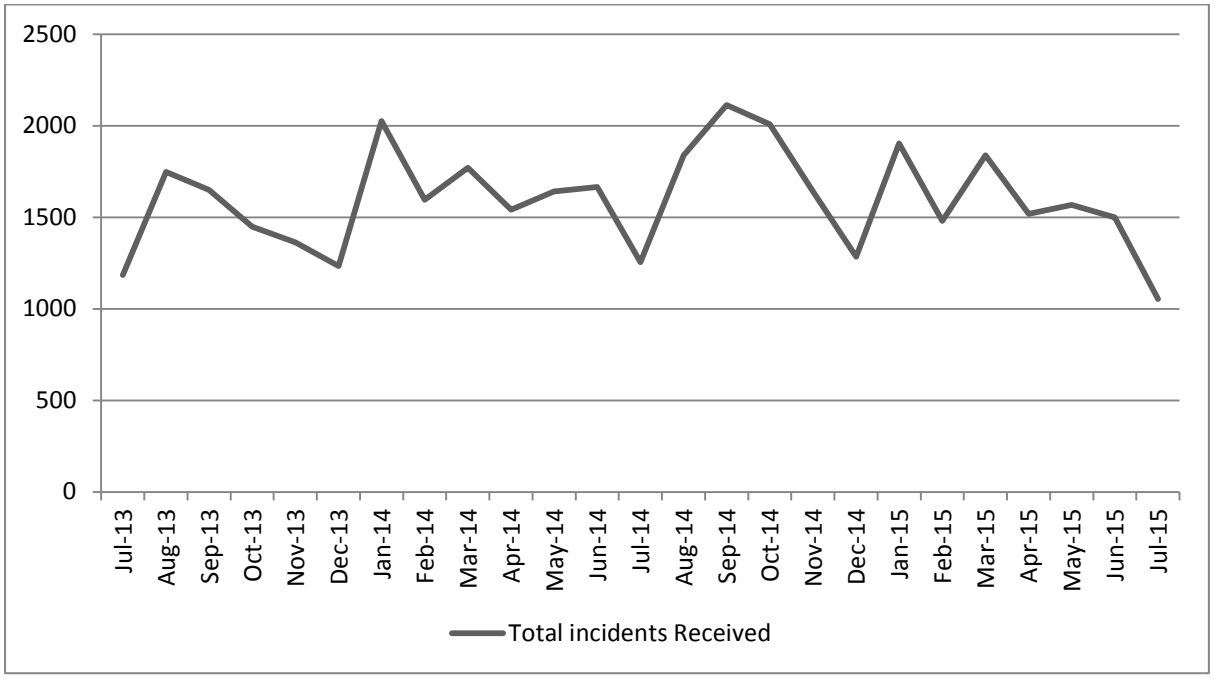
9.0 BACKGROUND PAPERS

9.1 None

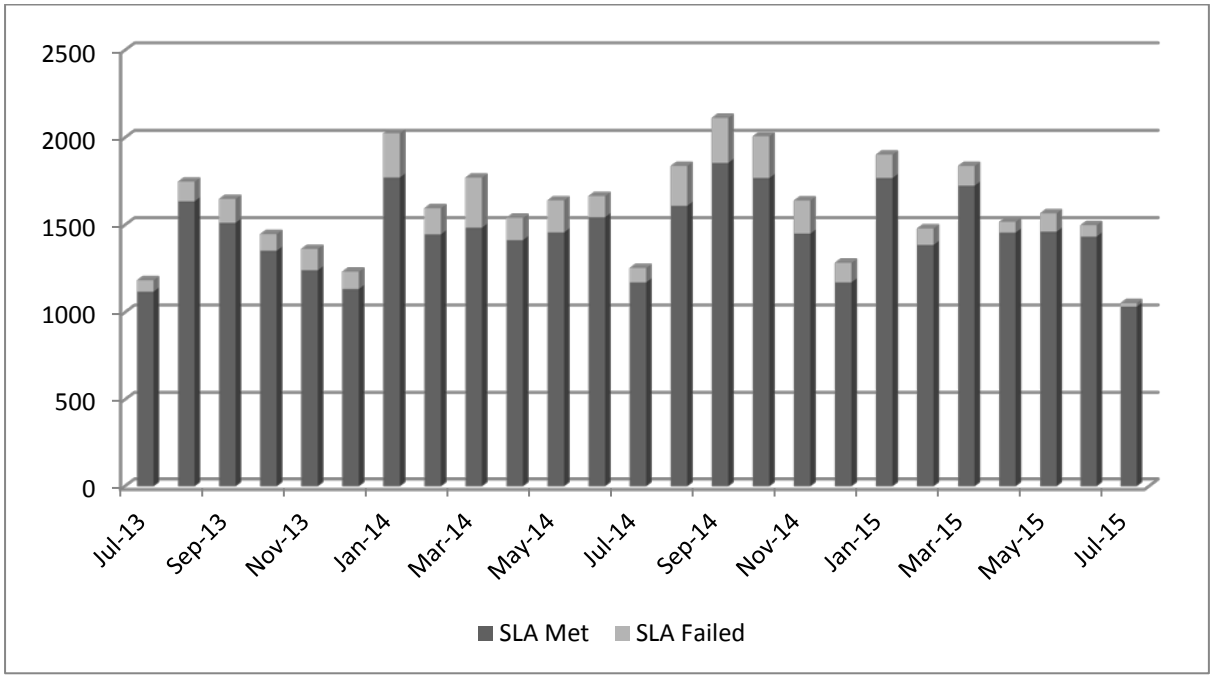
Appendix 1 – Performance Statistics

Servicedesk – Incidents

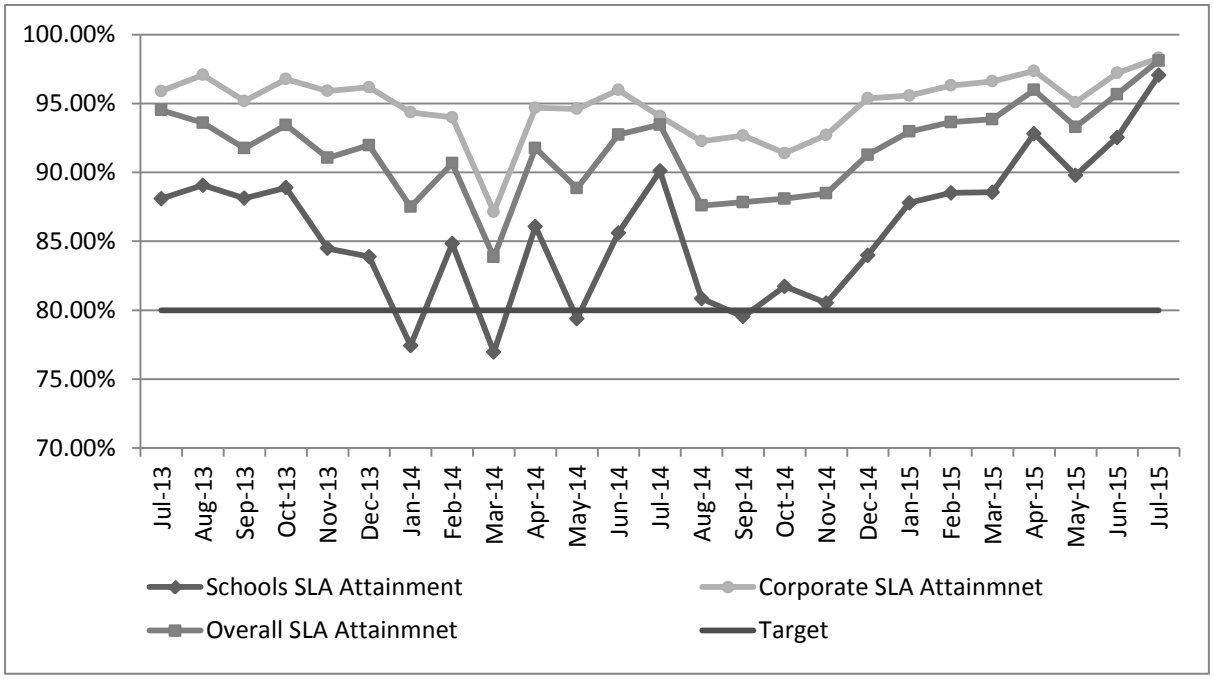
Incidents Received



Incidents Met/Failed within SLA



Monthly Service Level Attainment - Incidents



SLA Details

VIP Users

Priority	Target Resolution Time
Critical	3 hours
High	4 hours
Normal	7 hours
Low	21 hours
Long Term	No target

Standard Users

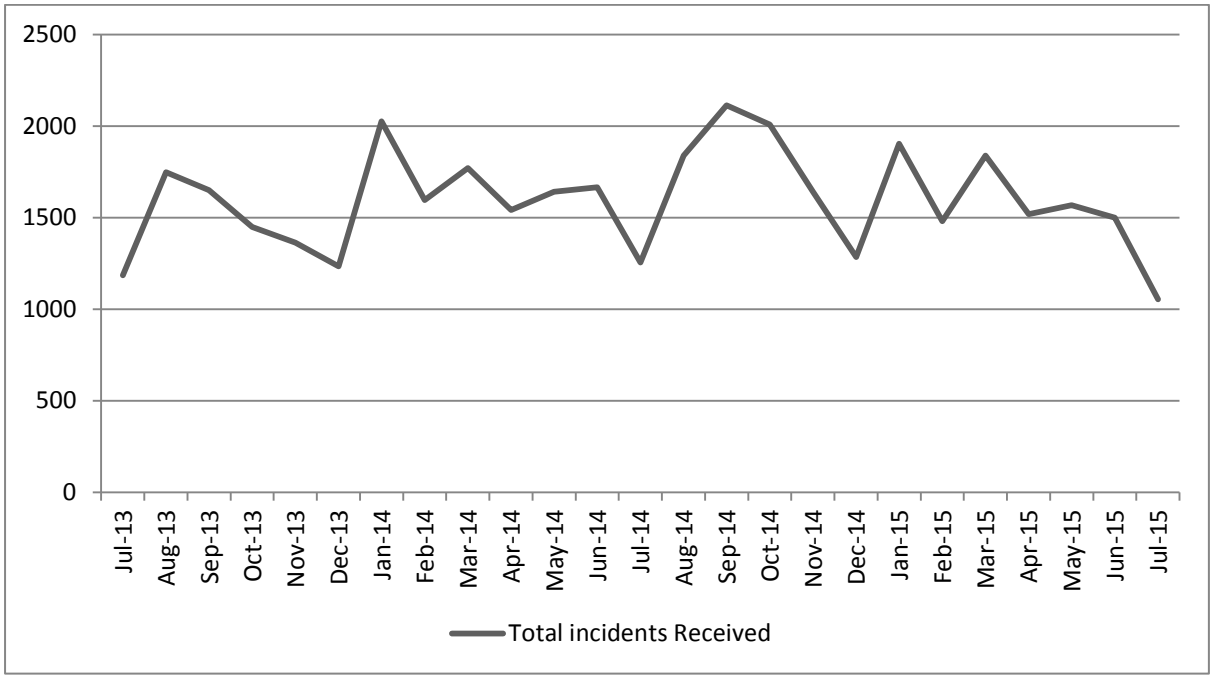
Priority	Target Resolution Time
Critical	4 hours
High	7 hours
Normal	21 hours
Low	35 hours
Long Term	No target

SLA Attainment is 80% of incidents resolved within Target Resolution Time.

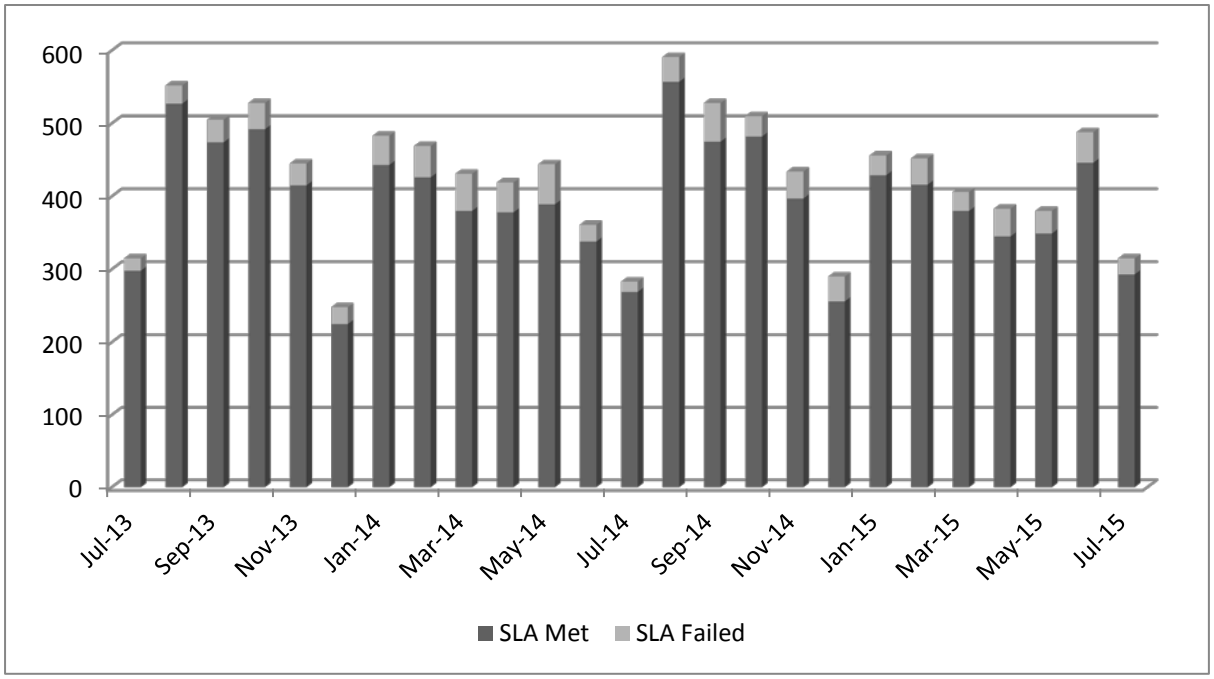
A typical Service request is unlocking a disabled user account or password, software errors, whiteboard and projector issues.

Servicedesk – Service Requests

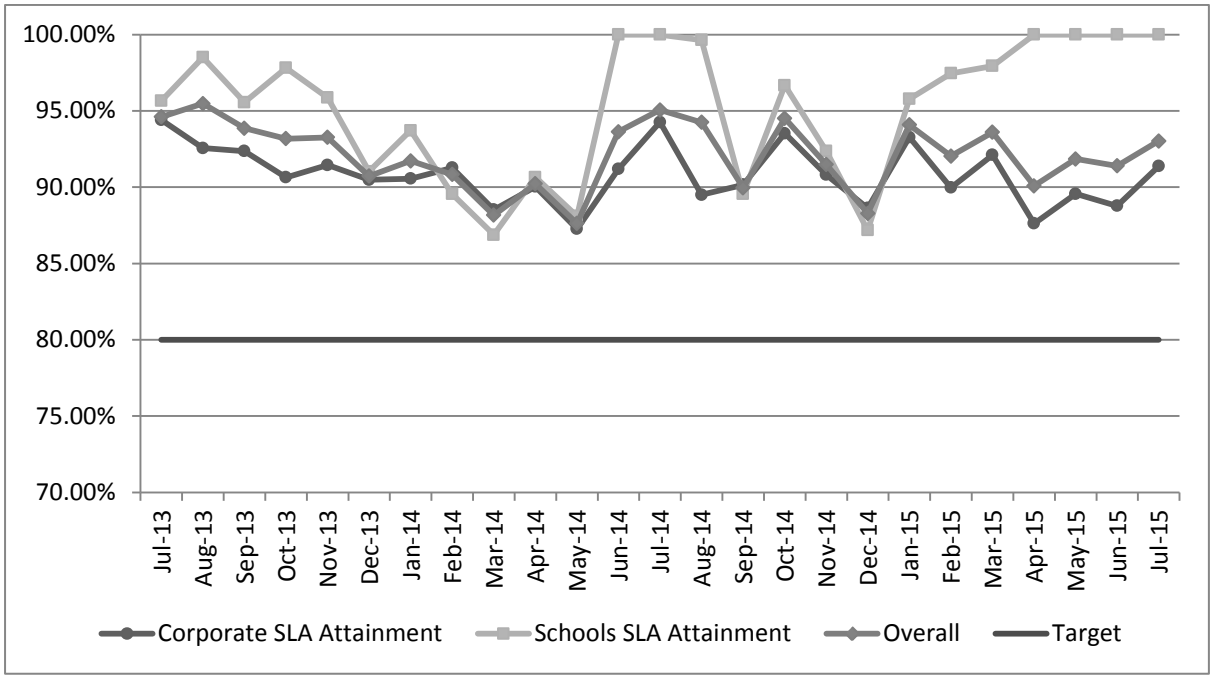
Service Requests Received



Service Requests Met/Failed within SLA



Service Level Attainment – Service Requests



SLA Details

Priority	Target Resolution Time
Critical	2 Days
High	5 Days
Normal	10 Days
Low	30 Days
Long Term	No target

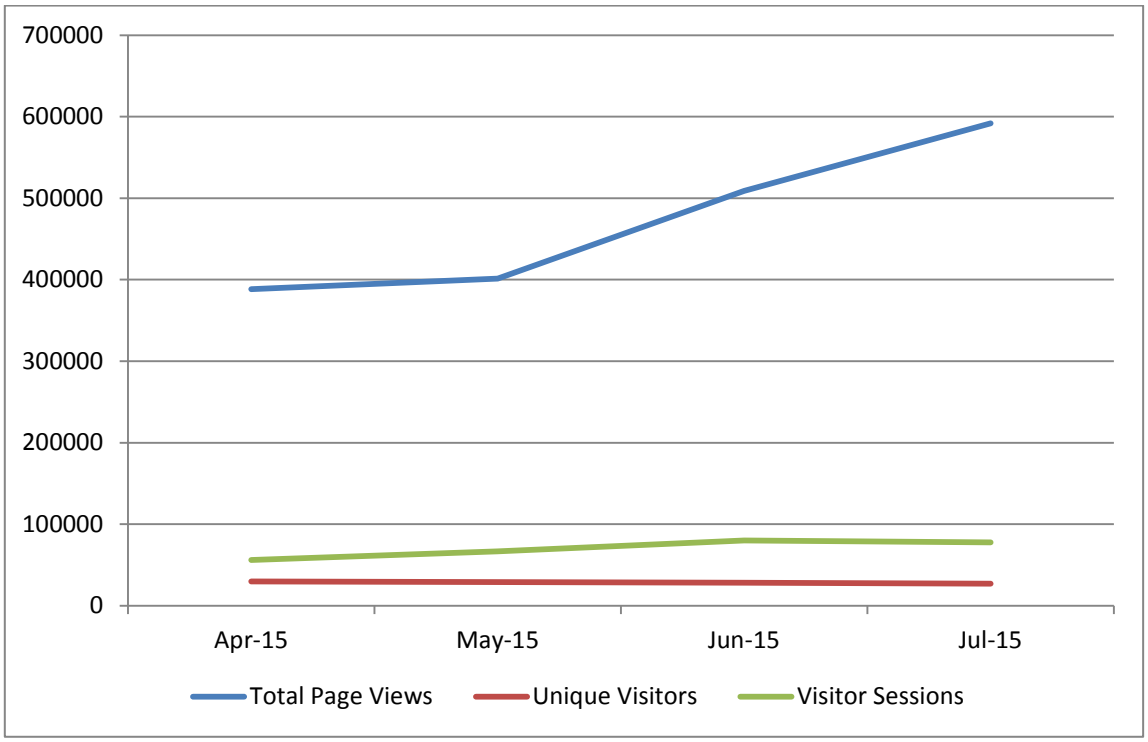
SLA Attainment is 80% of incidents resolved within Target Resolution Time.

A typical Service request is provision of a new user account, a new PC or Laptop, relocation of existing services.

Internet and Web Access

www.inverclyde.gov.uk – site statistics

Refreshed website launched May 15



	Apr-15	May-15	Jun-15	Jul-15
Total Page Views	388377	401122	508999	591627
Unique Visitors	29781	29101	28248	26948
Visitor Sessions	55928	66811	80088	77765

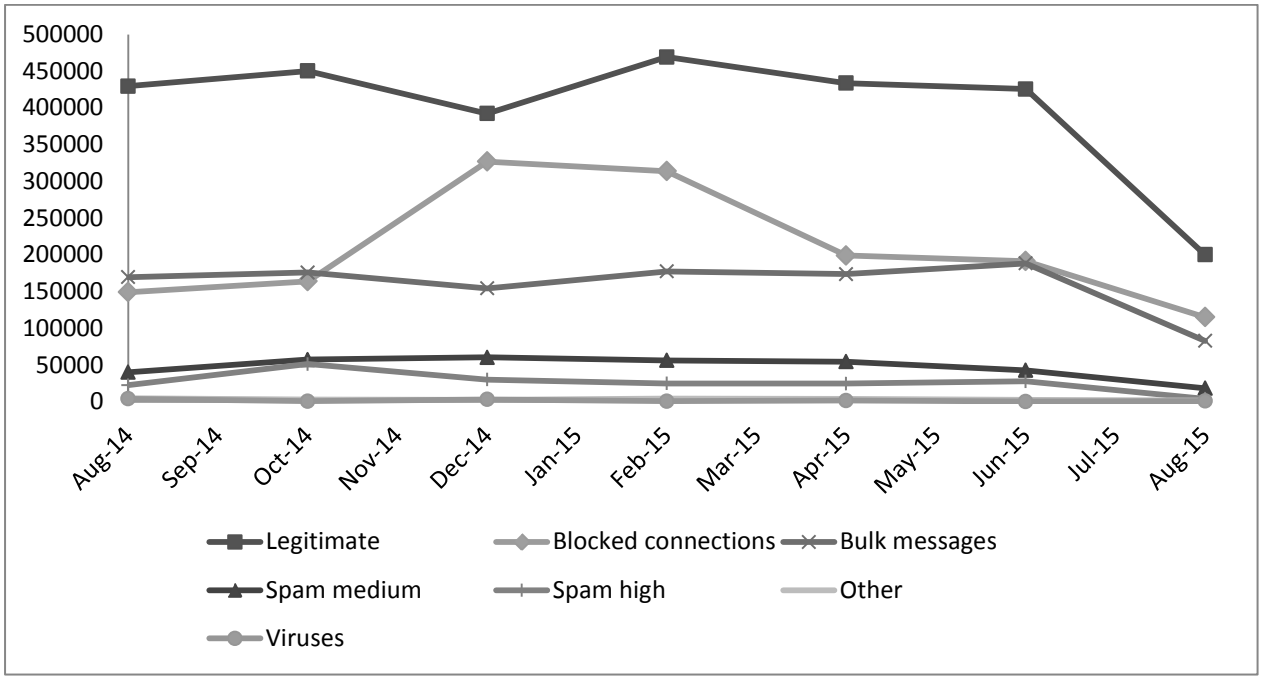
Page View: A single view of a single web page from an individual visitor to our site.

Unique Visitor: Unique IP (web) address to identify our viewers.

Visitor Sessions: The number of times a unique visitor returns to view the site after leaving for more than 20mins.

Email

Inbound Email Volumes – 52 Week Trend



	Aug14	Oct14	Dec 14	Feb 15	Apr 15	Jun 15	Aug 15
Legitimate	429585	450282	392228	469161	433666	425636	200277
Blocked connections	149205	164035	326972	314008	199091	191501	115282
Bulk messages	169814	176013	154473	177670	173955	188504	83056
Spam medium	40485	57590	60637	56479	54791	42942	18687
Spam high	22681	51428	30448	25197	24914	27960	4173
Other	4965	3360	2715	4461	3981	3014	1802
Viruses	4204	1069	3397	889	1800	561	1224
Total	820939	903777	970870	1047865	892198	880118	424501

Blocked connections – sources identified as being nodes where spam originates.

Bulk messages – messages with multiple recipients, usually marketing type emails

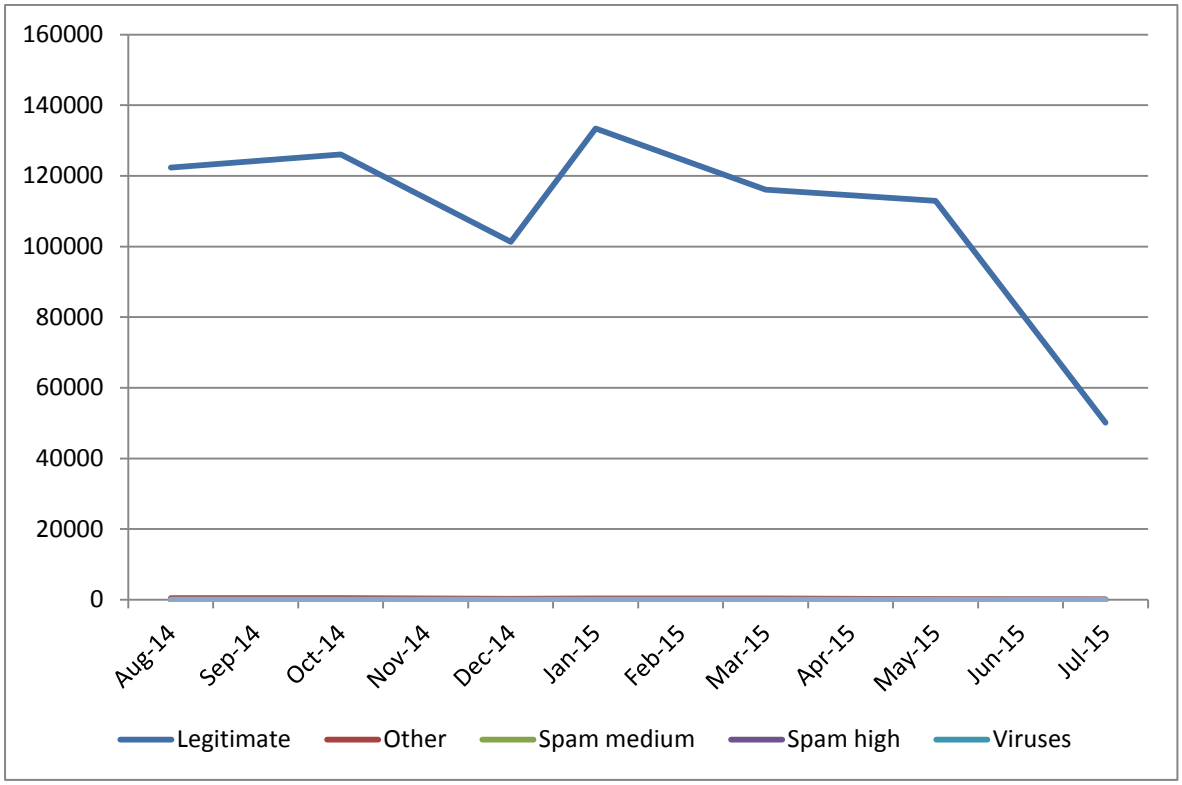
Spam medium – messages with a medium probability rating of being Spam – a message is forwarded to recipient asking if the email is to be released.

Spam high – messages identified as being with a high probability rating of being Spam – automatically quarantined.

Other – offensive or racist language, inappropriate content.

Virus – messages containing malicious software designed to disrupt system use or create a data breach.

Outbound Email Volumes



	Aug-14	Oct-14	Dec-14	Jan-15	Mar-15	May-15	Jul-15
Legitimate	122378	126096	101320	133414	116111	112960	50120
Other	437	431	249	344	336	235	107
Spam medium	2	3	12	6	27	14	10
Spam high	0	0	0	1	0	0	26
Viruses	0	0	0	0	0	0	2
Total	122817	126530	101581	133765	116474	113209	50265

Spam medium – messages with a medium probability rating of being Spam – a message is forwarded to recipient asking if the email is to be released.

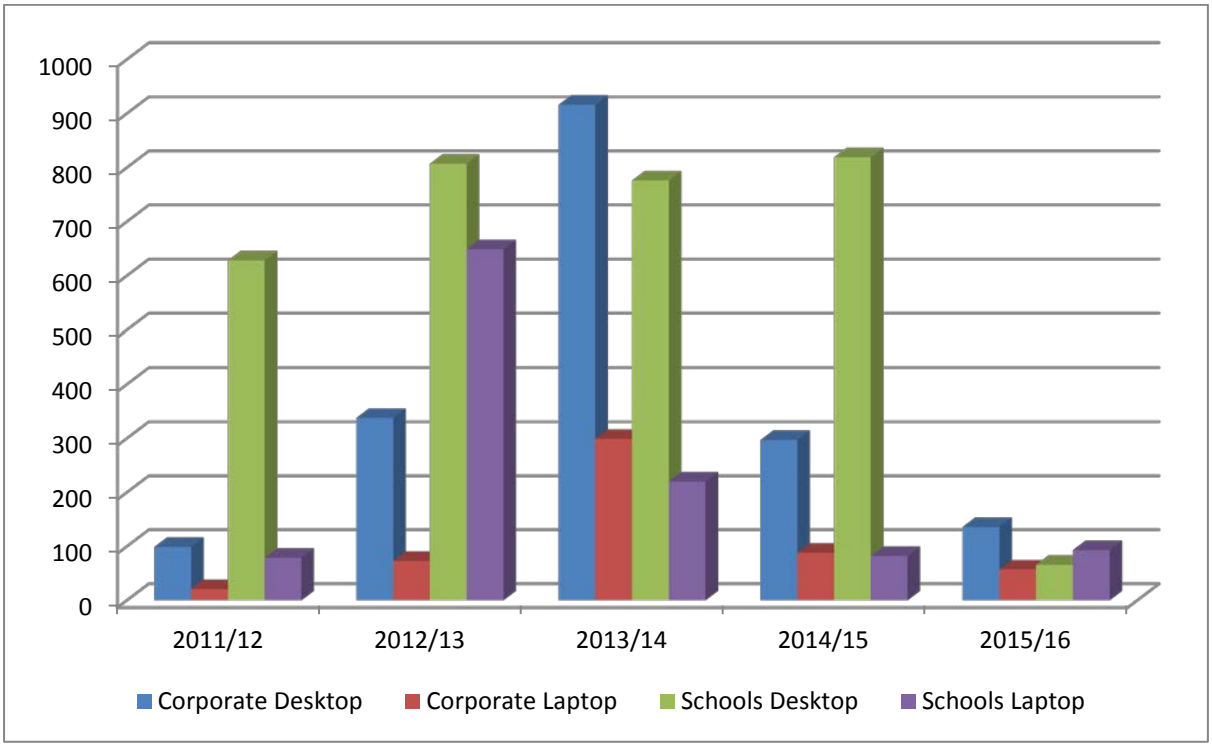
Spam high – messages identified as being with a high probability rating of being Spam – automatically quarantined.

Other – offensive or racist language, inappropriate content.

Virus – messages containing malicious software designed to disrupt system use or create a data breach.

Note. The majority of irregular messages detected are false positives. Legitimate reports containing potentially offensive language, tiles or contents of messages that have similar phrasing to typical bulk or spam emails.

PC Refresh programme



Year	2011/12	2012/13	2013/14	2014/15	2015/16
Corporate Desktop	99	338	916	297	136
Corporate Laptop	21	73	299	88	57
Schools Desktop	628	807	776	819	66
Schools Laptop	79	649	220	82	93

Appendix 2 – Projects Update

EDRMS

The Corporate Electronic Document Management System is now well established in Revenues and Benefits and the HSCP. Further opportunities are being explored in OD,HR & Communications. This project continues to drive efficiency opportunities for service and, dependent on appropriate value for money tests being achieved, could be further deployed across other Council Services.

As part of this process a review of network storage is being undertaken.

Scottish Wide area Network (SWAN)

The council has now formally become a member of SWAN following signing of the Membership Agreement and Commercial Contract with the SWAN Management Board, and their suppliers Capita IT Systems. Full project planning has now commenced, a High Level Design document has been agreed and implementation is scheduled for December 2015 – April 2016.

The ICT Operations Manager is currently attending the SWAN Board on behalf of the council.

Digital Access Strategy

Customer Services – Kana Upgrade

All elements of the upgrade to the Kana Customer Services systems are now complete. A target go-live date of September 2015 is planned and ICT and CSC have completed the relevant training and implementation plans

The Self Service Portal (SSP) will be accessible from the main council website and offer citizens access to any process in the core KANA system, alongside existing face to face and telephone channels. There is work ongoing with e the Improvement Service and the wider Scottish Public Sector to develop the MyAccount service that will allow citizens to securely log-on to any public website and create accounts similar to internet banking or ecommerce sites.

Employee Mobile is an app for mobile devices which enables council officers to be notified, take ownership and expedite cases logged in the KANA system. There have been initial discussions with a number of services to implement pilot projects.

Citizen Mobile is also an app for mobile devices which offers similar functionality to the Self Service Portal. This will provide another route to services for citizens. The app takes advantage of the GPS positioning and camera technology inherent in the devices to capture rich and accurate data to attach to the case created in KANA system.

Schools Online Payments

ICT Services are working with Education Services and the Improvement Service to develop a business case to implement a Schools Online Payment System. This would allow parents and guardians the

opportunity to pay for a wide range of services such as school meals, trips, uniforms etc. to be paid via an online portal.

Council Website

The refreshed website was launched in May 2015. A modest increase I the number of unique visitors has been recorded however there has been a notable increase in page views, which would seem to indicate that visitors are making greater use of a the site during their visits. Further developments such as the Customer Self Service and additional Online payments should drive more traffic to the site.

GIS/Mapping Services

The Council GIS and Mapping Systems are being upgraded to provide a better user experience allowing more Council Services, and ultimately Council customers the ability to use interactive maps to plan, report issues and consume services.

Secure GCSX Mail

A contract for the provision of a new Secure Email facility has been agred with Vodafone UK. A target implementation date of September 2015 is planned.

PSN

The PSN accreditation process is underway for 2015/16. ICT Service Manage met with the UK Cabinet office in June 2015 to discuss current and future compliance regimes and provide an update on the Council's ongoing commitment the PSN Accreditation process.

The IT Health Check & Network Penetration Test will be carried out by independent external IS Security Auditors in early September, prior to the reaccreditation documentation submission scheduled for October 2015.

A new Physical security of IT Systems policy is to be considered at Policy and resources Committee.

Email and Email Archiving Upgrade

The current Email System was implemented in 2007. A project to upgrade to the latest version has been implemented. External partners are working with ICT Services to design and deliver the project.

The Email Archiving system is also scheduled for upgrade and this will be completed prior to the upgrade.

BYOD

ICT Service has completed the necessary infrastructure works to support the schools Bing Your Own Device Project. The schools have been working with ICT and Education Services to allow BYOD to be introduced early in the new school year.

Information Governance & Management Framework

Policy for the Physical Security of ICT Infrastructure

Version 0.1

Produced by:
ICT Services
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

23/07/2015

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER

THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR CD/DVD.

DOCUMENT CONTROL

Document Responsibility		
Name	Title	Service
Allan McDonald	Operations Manager	ICT

Change History		
Version	Date	Comments
0.1	23 July 2015	Draft

Distribution		
Name	Title	Location

Distribution may be made to others on request

1. Introduction

1.1 Inverclyde Council is required to take appropriate measures, both in law and in best practice, to ensure that access to data stored on its ICT infrastructure is protected, managed and controlled both electronically and physically.

1.2 The Council has identified key points on our ICT network that requires additional physical security and control procedures to ensure access is restricted only to those staff or individuals who have a legitimate requirement.

2. Aims and principles

2.1 Any loss of access to information or interference with its integrity could have a significant effect on the operational efficiency of the Council and could put it at risk of sanction or prosecution from the Information Commissioner's Office (ICO). It is therefore essential that the confidentiality, integrity and availability of all information systems are maintained at a level, which is appropriate to the Council's needs and obligations.

2.2 This Policy aims to establish a set of Physical Security Standards and Access Control guidelines for locations that are used for the purpose of housing ICT Servers, Appliances, Network Storage, Network Switches, and termination points for Network Cabling Infrastructure (Fibre Optic and Copper Cabling Patch Panels) and any other relevant ICT infrastructure.

3. Scope

3.1 This policy applies to all users. The definition of a user includes all Services, Elected Members, Employees of the Council, Pupils, contractual third parties and agents, or any other individual or organisation who has been granted access to the Council's ICT systems and services.

3.2 This policy identifies and applies to the following physical locations/entities in all locations operated by the Council in which ICT Services are provided including offices, schools libraries and third-party facilities:

- Data Centre (DC) – Primary Physical Location of the Council's Server and Network Infrastructure.
- DR Data Centre (DRDC) – Secondary Physical location of core backup services to the DC.
- Data Hub – Remote/Offsite Location used for the local colocation of ICT Services – typically this will be a small room with one or more data cabinets

- Data cabinet – Physical Storage Unit – typically used to host network Switches and patch panels – ideally hosted within a data hub, but often located in general office areas

4. Responsibilities

ICT Services is responsible for ensuring these policies are implemented. Departments and Services are responsible for ensuring that all staff members within their organisations are aware of, and comply fully with, these policies.

5. Data Centre and DR Data Centre

5.1 The Data Centre is located in a secure area of the Greenock Municipal Buildings (GMB). Access to this area is controlled by an electronic access control system and an extensive CCTV system is in place. Access is restricted to authorised ICT staff and those staff/contractors directly responsible for the provision of ICT Services to the Council and its partners. Logs are stored on the access control system of all access to this area.

5.2 The DR data Centre is located within a data hub school building in Port Glasgow. It is currently managed in conjunction with facilities management staff within the school. Access is restricted to authorised personnel only. A CCTV Camera monitors access.

6. Physical Security and Access Control

6.1 The Council recognises it may not be possible or practical for all current locations to meet all of the requirements of this policy. However all practical steps must be taken to mitigate any potential access issues. **As a minimum**, the following steps must be taken to ensure the best possible level of security at each location

6.2 Data Hubs – Data Hubs are for the sole use of ICT Services for the provision of secure network services. They must not be used for storage of non IT equipment. Access must be restricted to ICT Staff and Facilities Management Staff approved by the ICT Operations Manager. **Unauthorised access will be treated as a potential Data Breach and will be subject to the terms and procedures in the Council's Data Protection and Acceptable Use of Information Systems policies.**

6.2.1 Where practical additional Electronic or Physical Coded Locks will be deployed. Access to the codes or through the electronic control system must be restricted to staff agreed and approved by ICT Services. A CCTV Camera will be deployed where possible.

6.2.2 Where it is not possible to deploy additional door controls, access to keys must be restricted to appropriate ICT and Facilities Management Staff.

6.2.3 Appropriate signage indicating restricted access and the presence of CCTV will be displayed in all locations. Where possible "no access to unauthorised personnel" signage will be displayed on all doors.

6.3 Data Cabinets – All existing Data Cabinets must have a suitable lockable door and all appropriate panels installed. No access to components inside the cabinet should be available without unlocking the door/removing the security panels.

7. New Builds/Refurbishment

7.1 ICT Services and Legal and Property Services have a longstanding and effective agreement on the provision of ICT Service to new build or refurbished properties. This policy reinforces the requirement for both ICT Services and any service involved in the commission of new Council properties to work in cooperation to ensure that the appropriate security standards are met.