

Meet the new candidates

Nominations for General Election candidates closed this week, and the SNP has reselected all sitting SNP MPs – [the hardest working politicians at Westminster](#).

We've also selected five brand new candidates to help protect Scotland from the dangers of an unopposed Tory government at Westminster.

Meet your new SNP candidates.

I've told Britain's property developers: if you won't build houses, the Lib Dems will

The Conservative government has given developers a carte blanche to play the property market at the expense of our citizens. And now the country's in crisis.

Not enough homes. Properties sitting empty. Exorbitant prices. The market is closed and exclusive: a fat cats' game. That's not good for people and it's not good for business.

Today the Lib Dems are laying down the law to developers: **unless you build the homes that Britain needs, we will.**

We're tired of the commercially unsound and short-sighted greed of developers, who buy up local authority land and sit on it until it appreciates. We're tired of absent foreign investors, who's attractive up-front cash is a false economy – contributing nothing to the improvement of the surrounding public realm.

The Lib Dems are taking decisive action on the housing crisis.

As a modern, pro-business party, we think commercial sense and social justice go hand in hand. That's why we've put a progressive housing package at the heart of our new manifesto. It will include: building 300,000 homes a year by the end of the next parliament and giving local councils the power to charge absentee landlords up to 200% council tax on empty homes.

Why prioritise housing?

Making sure that the housing market is both profitable and socially beneficial is just pure good sense. But I also have personal reasons for

standing behind this issue. As a teenager, I was inspired to get into politics by watching Cathy Come Home – a heartbreaking film about a couple who were made homeless – and I joined the housing charity Shelter as a result.

As an MP, I've seen first-hand the misery caused not having a proper home. For many people in the next generation, it is virtually impossible to get on the housing ladder. I think they deserve a helping hand.

If you want a government who will fight for everyone's basic human need for shelter, who has the commercial clout to unpack the property monopolies which hold the market in a vice, then add your name here and say you're voting to change Britain's future on Thursday 8th June:

[Labour calls for action over NHS cyber-attack](#)

Jonathan

Ashworth, Labour's Shadow Health Secretary, has today written to Jeremy Hunt condemning "the cyber criminals whose flagrant disregard for our health service has placed patient wellbeing at risk".

Jonathan

Ashworth said:

"The incident highlights the risk to data security within our modern health service and reinforces the need for cyber security to be at the heart of government planning.

"As

Secretary of State, I urge you to publicly outline the immediate steps you'll be taking to significantly improve cyber security in our NHS. The public has a right to know exactly what the Government will do to ensure that such an attack is never repeated again."

The

letter from Labour's Shadow Health Secretary, calls on the Government to set out:

.

Why

NHS organisations failed to act on a critical note from Microsoft two months ago?

.

What additional resources are being given to the NHS to bring the situation under control as soon as possible?

.

What arrangements are currently in place to protect our NHS, and its sensitive data, against cyber-attacks?

.

Whether the Government will launch a full, independent inquiry into the events of yesterday?

.

Reassurance for patients that no patient data has been accessed or compromised in yesterday's attack?

Ends

Notes

to editors:

.

Please see below for full text of the letter:

Dear
Secretary of State,

I am writing to ask for urgent clarification regarding yesterday's major ransomware attack on our NHS. I hope you'll join me in condemning the actions of the cyber criminals whose flagrant disregard for our health service has placed patient wellbeing at risk.

As you know, the attack has had a serious impact on services, with some hospitals diverting emergency ambulances and cancelling elective operations. A large range of IT services have been affected, including pathology test results, x-ray imaging systems, phone and bleep systems, and patient administration systems.

In total more than a third of NHS Trusts have been impacted, and NHS England has consequently declared a Major Incident. This is terrible news and a real

worry
for vulnerable patients and our hardworking staff.

The
incident highlights the risk to data security within our modern health
service
and reinforces the need for cyber security to be at the heart of government
planning.

As
Secretary of State, I therefore urge you to publicly outline the immediate
steps you'll be taking to significantly improve cyber security in our NHS.
The
public has a right to know exactly what the Government will do to ensure that
such an attack is never repeated again.

However,
this is not the first time NHS Trusts have been attacked. In February,
Freedom
of Information Requests found that 79 English Trusts, more than 33 per cent,
had suffered ransomware attacks since June 2015.[\[1\]](#)

For
example, Imperial College Healthcare NHS Trust was attacked 19 times in 2016,
and the Leeds Teaching Hospital faced five attacks in the past year.[\[2\]](#) In
November, a major ransomware
attack on the Northern Lincolnshire and Goole Trust affected three hospitals,
forcing the cancellation of hundreds of routine operations and outpatient
appointments.[\[3\]](#)

As
recently as in January, the largest NHS Trust in England, Barts Health Trust,
was infected with a ransomware virus affecting thousands of sensitive
files.[\[4\]](#)

I am
therefore extremely concerned that extensive warning signs appear to have
been
ignored by yourself and your department.

Moreover,
your own colleague Ben Gummer, the Minister for the Cabinet Office, warned in
October that "large quantities of sensitive data" held by the NHS and the
Government were being targeted by hackers, with the potential for significant
disruption.[\[5\]](#)

Speaking
about the threat to the health service, Mr Gummer stated: "The Government has
a
clear responsibility to ensure its own systems are cyber secure. We hold and
the rest of the public sector- including the NHS- hold large quantities of
sensitive data and provide online services relied on by the whole

country.”[\[6\]](#)

Furthermore,
in March a joint report from the National Cyber Security Centre (NCSC) and the
National Crime Agency (NCA) warned that cyber-criminals could increasingly lock
computers, phones and watches to run cyber extortion and blackmail rackets.

At the
time, Ian Levy, technical director of the NCSC, warned that the best defence
against ransomware was to ensure software on devices was up to date.[\[7\]](#)

However,
it appears that many of those hospitals affected by yesterday’s attack had
not
updated their Windows operating systems to include a security patch. This
unacceptable cybersecurity neglect has clearly made the NHS extremely
vulnerable to an attack.

NHS

Trusts have been running thousands of outdated and unsupported Windows XP
machines despite the Government ending its annual £5.5 million deal with
Microsoft, which provided ongoing security support for Windows XP, in May
2015.[\[8\]](#)

It
effectively means that unless individual Trusts were willing to pay Microsoft
for an extended support deal, since May 2015 their Operating Systems have
been
extremely vulnerable to being hacked.

Given

your Government’s sustained underfunding of our NHS it is of little surprise
that many Trusts have reported taking minimum action. Indeed, research
through
previous FOIs has found that at least seven NHS Trusts, which treat more than
two million Britons, spent nothing at all on cyber security infrastructure in
2015.[\[9\]](#)

This is
extremely serious and as Shadow Secretary of State of Health I share the
public’s concern at these revelations.

Yesterday’s

attack is unprecedented in scale, but it is abundantly clear that our NHS
should have been better prepared for ransomware attacks.

Therefore,

will you firstly explain why NHS organisations failed to act on a critical
note
from Microsoft two months ago?

Secondly,
what additional resources are you giving the NHS to bring the situation under control as soon as possible?

Moreover,
will you clarify publicly what arrangements are currently in place to protect our NHS, and its sensitive data, against cyber-attacks? Will you ensure that every single NHS organisation receives an on-site assessment from CareCERT to improve security?

Will you
additionally launch a full, independent inquiry into the events of yesterday?

Finally,
will you reassure patients that no patient data has been accessed or compromised in yesterday's attack?

Secretary
of State, the prevalence and sophistication of cyber-attacks on our NHS is only
set to increase. I therefore urge you to take immediate action so that a
crisis
on this scale is never repeated again.

Yours
sincerely,

Jonathan
Ashworth

Shadow
Secretary of State for Health

[1] <https://www.ft.com/content/e96924f0-3722-11e7-99bd-13beb0903fa3>

[2] <https://www.ft.com/content/b9abf11e-e945-11e6-967b-c88452263daf>

[3] <https://www.ft.com/content/b9abf11e-e945-11e6-967b-c88452263daf>

[4]
<http://www.telegraph.co.uk/news/2017/01/13/largest-nhs-trust-hit-cyber-attack/>

[5]
<http://www.telegraph.co.uk/news/2016/10/31/nhs-at-risk-of-cyber-attacks-minister-says-as-he-warns-hackers-a/>

[6]
<http://www.telegraph.co.uk/news/2016/10/31/nhs-at-risk-of-cyber-attacks-minister-says-as-he-warns-hackers-a/>

[7]
<http://www.telegraph.co.uk/news/2017/03/14/smartphones-tvs-watches-could-held>

[-ransom-hackers-cyber-security/](#)

[8]

<http://www.silicon.co.uk/security/nhs-hospitals-data-risk-outdated-windows-xp-201761>

[9] <https://www.ft.com/content/b9abf11e-e945-11e6-967b-c88452263daf>

Flights disrupted by drone at SW China airport

More than 200 flights were disrupted due to an unauthorized drone flying around an airport in southwest China's Chongqing Municipality Friday evening.

Flights to and from Chongqing Jiangbei International Airport were affected from 7:20 p.m. Order was restored at 9:37 p.m., but 34 minutes later the drone appeared again.

More than 40 flights were forced to land at alternative airports, while over 60 were canceled and another 140 were delayed, affecting over 10,000 passengers.

This was the second time an unauthorized drone has caused disruptions at the airport this week. On Tuesday, 12 flights were forced to land elsewhere.

As privately-owned drones have become increasingly popular in China, several airports have experienced flight disruptions due to illegal drone activity, which poses a threat to aviation safety.

In late April, four drones were illegally flown over Chengdu Shuangliu International Airport in southwest China's Sichuan Province, which forced 58 flights to land at alternative airports, four flights to return to their departure airport, and more than 10 to be canceled.

Since February, Kunming Changshui International Airport in Yunnan Province has reported at least seven drone disruptions. Local police have launched investigations.

Temporary Traffic Order – Roseangle



From the City Council :

THE ROAD TRAFFIC REGULATION ACT 1984 : SECTION 14(1)

THE DUNDEE CITY COUNCIL AS TRAFFIC AUTHORITY being satisfied that traffic on the road should be prohibited by reason of SGN service connection works being carried out HEREBY PROHIBIT the driving of any vehicle in Roseangle (between Perth Road and Seabraes Court), Dundee.

This notice comes into effect on Monday 22 May 2017 for 5 working days.

Pedestrian thoroughfare will be maintained.

Alternative routes are available via Perth Road / Windsor Street / Magdalen Yard Road.

For further information contact 433082.

Mike P Galloway
Executive Director of City Development
Dundee City Council