

# Whole disk encryption in Oxford

Tony Brett

Head of IT Support Staff Services

IT Services

University of Oxford

ICT Forum Conference

10 July 2014

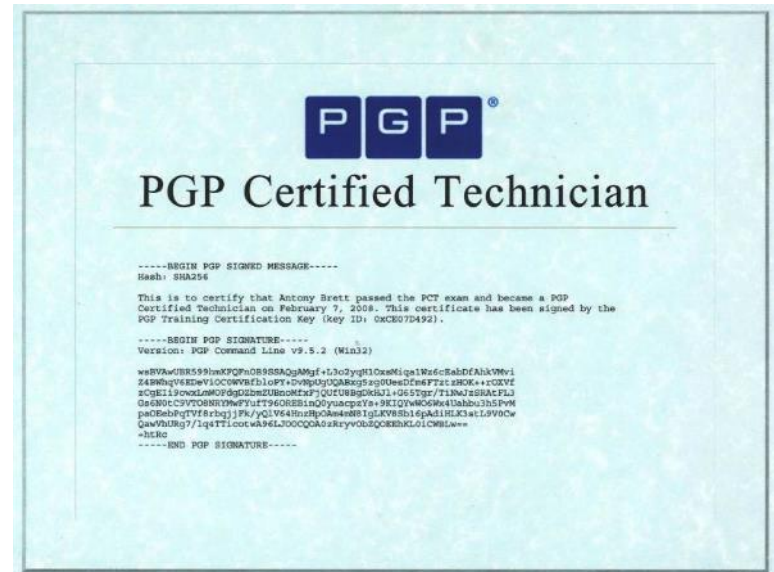


# We'll talk about these things

- How it all started
- Why the University wants to do this
- Essentials for the service
- Support Processes
- The WDE project
- How ITSS are crucial to this service
- Some facts and figures
- The future
- Q&A

# How it all started

- IT Services has been researching this for some time
- Jon Ashton and I were trained at PGP Corporation in Offenbach in 2008
- Ignoring information security no longer an option



# The University wants to do this because...

- Easy to lose portable computers
- Data loss is a big risk – WDE reduces
- University has statutory duty to protect its data and that of its staff and students
- Data loss = reputation damage, large fines and more
- The ICO has a lot of power
  - Fines up to £500,000 for serious breaches of the Data Protection Act and Privacy and Electronic Communications Regulations.
  - See <http://ico.org.uk/enforcement/fines>



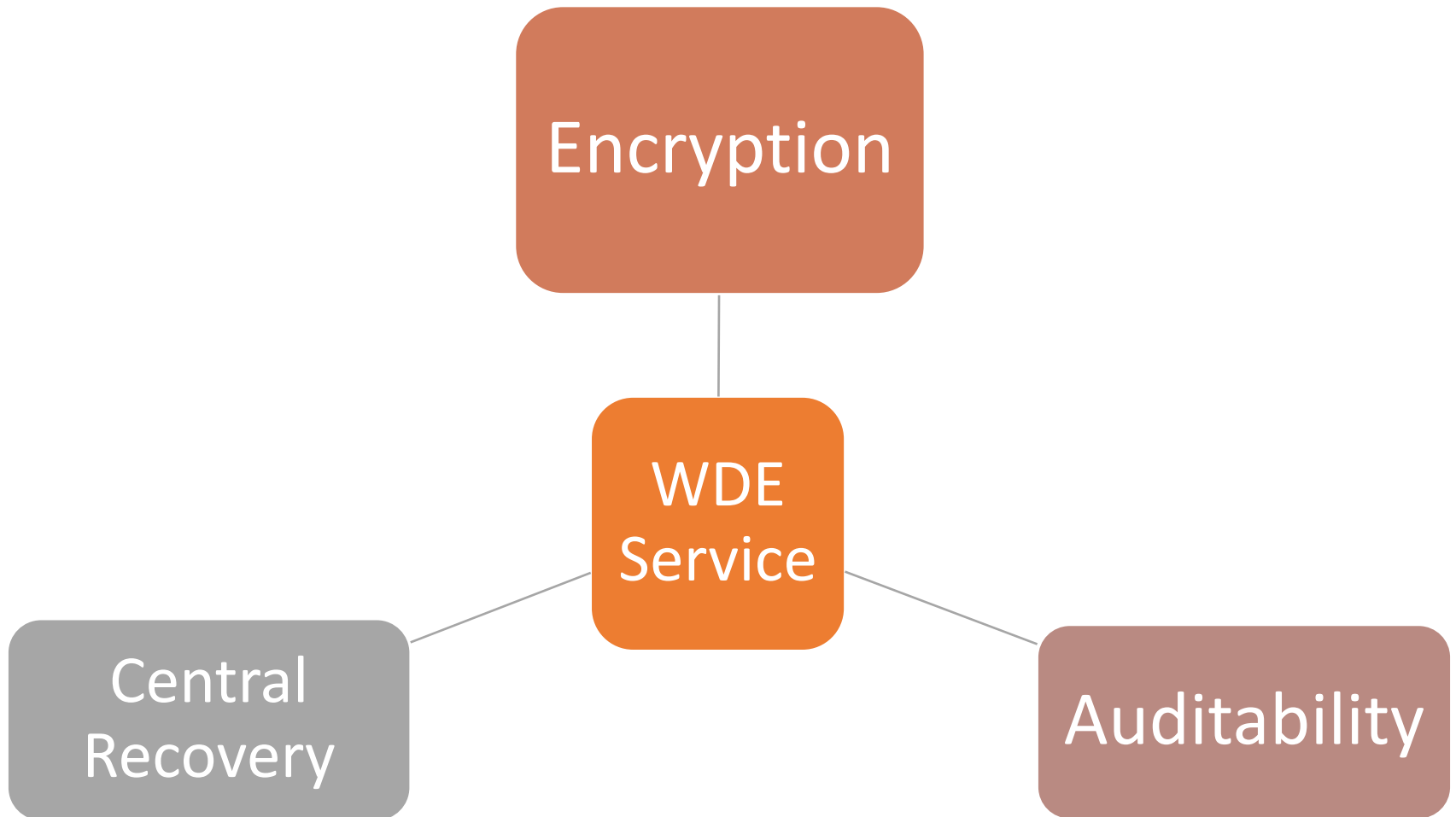
# Can we use bitlocker or file vault?

- These offer encryption but don't scale to the enterprise very well
- Similar products available



- You really need recoverability and audit capability

# The Registrar had three essential requirements



# Symantec acquired PGP in 2010

- University had decided to use the PGP Universal Server and PGP desktop solution
- Became Symantec Encryption Server and Symantec Encryption Desktop
- WDE project launched in Summer 2013
- Required to support Mac, PC, Linux(s)



# WDE project objectives

- The ability to perform whole disk encryption on fixed and removable (disk) drives
- Centralised policy enforcement
- Recovery from forgotten passphrases even when user is away from “home”
- Audit trails of encryption, decryption, recovery and policy compliance



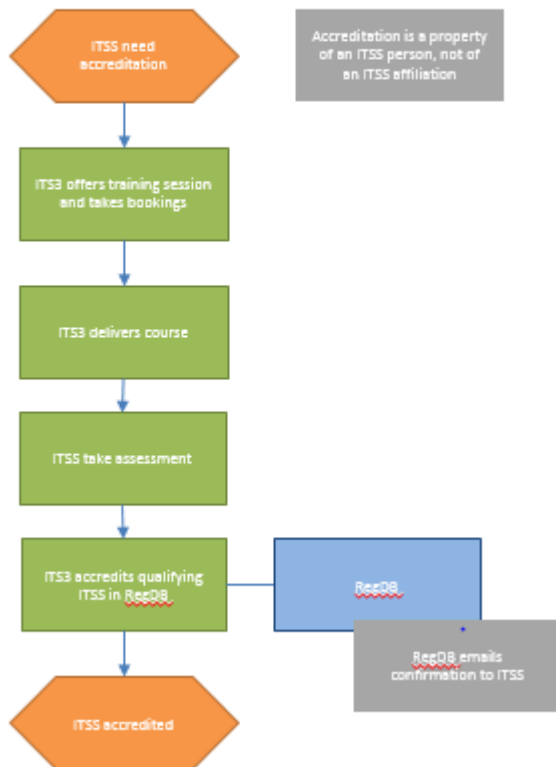
# WDE project scope

- Implementation of the Symantec Encryption Management Server (WDE infrastructure)
- Implementation of any necessary charging mechanism
- Service provided to ITSS to enable them to implement WDE within their departments
- Implementation of a testing environment
- Provision of user documentation for local ITSS
- Provision of second line support (via local ITSS)
- Training of ITSS to provide first line support
- Purchasing of initial 500 client licences
- Design of the service work packages
- De-commissioning of the pilot service

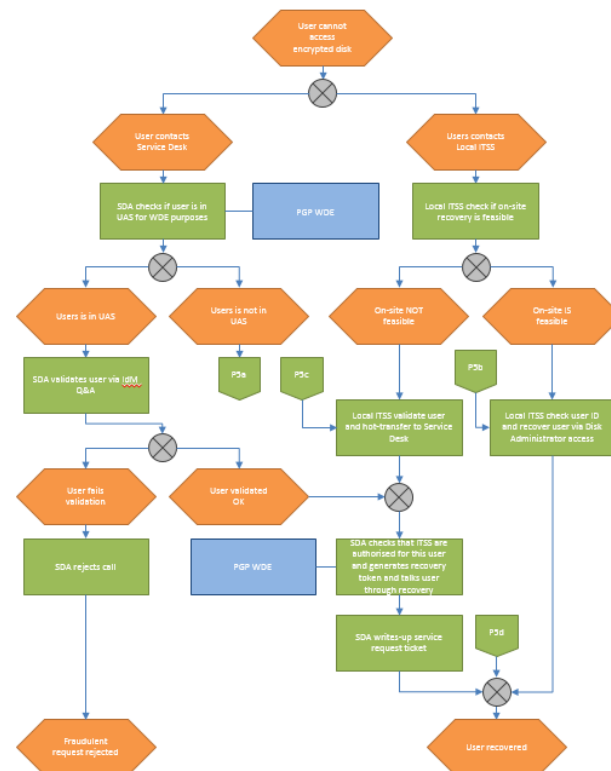
# Process is important to ensure security is not breached

- John Ireland, as service owner, did some designs

## P19. ITSS Accreditation

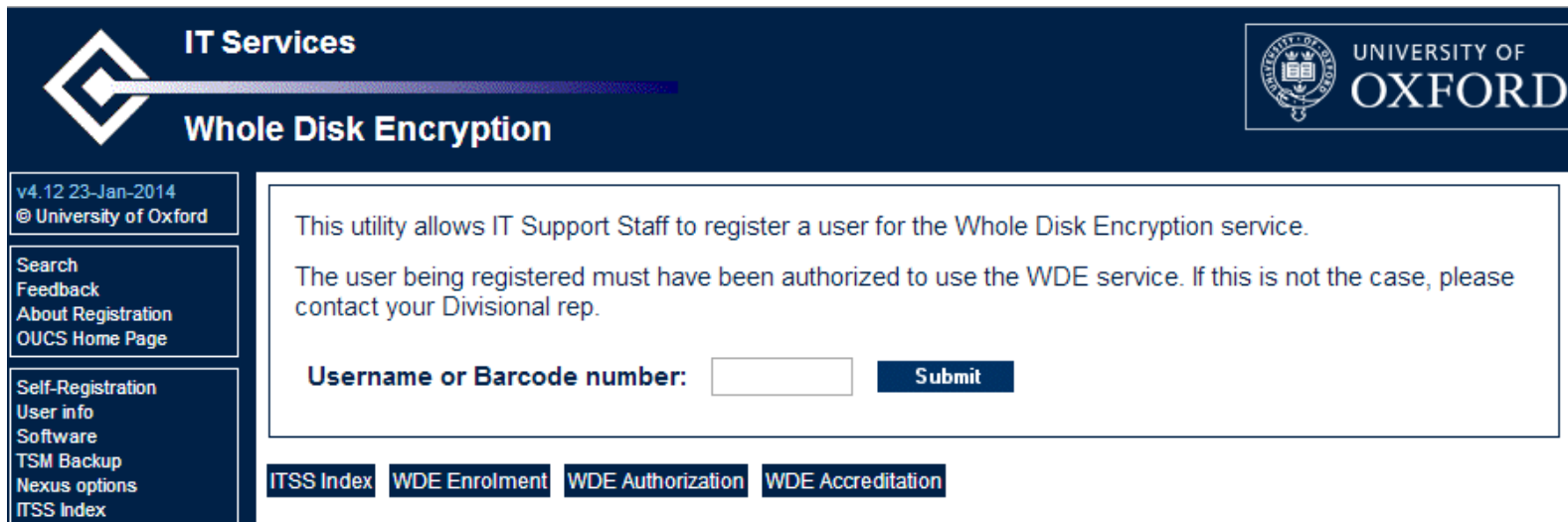


## P5. Issue Recovery Token



# Terminology must be clear

- Authorise = allow a particular user to be enrolled
- Enrol = set up user on back end so the can set up encryption
- Accreditation = Give ITSS the ability use the Enrolment tool



The screenshot shows a web page for 'IT Services' at the University of Oxford, specifically for 'Whole Disk Encryption'. The page includes a navigation menu on the left with links for Search, Feedback, About Registration, OUCS Home Page, Self-Registration, User info, Software, TSM Backup, Nexus options, and ITSS Index. The main content area contains a registration form with a text input field for 'Username or Barcode number' and a 'Submit' button. The footer of the page features a navigation bar with links for ITSS Index, WDE Enrolment, WDE Authorization, and WDE Accreditation.

**IT Services**

**Whole Disk Encryption**

UNIVERSITY OF OXFORD

v4.12 23-Jan-2014  
© University of Oxford

Search  
Feedback  
About Registration  
OUCS Home Page

Self-Registration  
User info  
Software  
TSM Backup  
Nexus options  
ITSS Index

This utility allows IT Support Staff to register a user for the Whole Disk Encryption service.


The user being registered must have been authorized to use the WDE service. If this is not the case, please contact your Divisional rep.

Username or Barcode number:  **Submit**

[ITSS Index](#) [WDE Enrolment](#) [WDE Authorization](#) [WDE Accreditation](#)


# ITSS training started...

- First session in November 2013
- About an hour of instruction
- Some practical work testing encryption
- A short test executed on Weblearn

 **Edit Assessment**

Type


Test  
 Assignment


 [Change to Survey](#)


Points

This Test is worth points.

Title


 [Edit Instructions](#)

 [Manage Parts](#)

 [Set Options](#)

Questions

This Test is locked: questions may not be added or removed.

| Order  | Description  | Type |
|--|--------------|------|
|  Part 1 | Test content |      |
| <input type="checkbox"/> 1 ▾   | Random Draw  | Draw |

Total Questions: 10  
Total Points: 10.0

(Optional) a percentage that represents the pass mark for this assessment.

# A big push in UAS

- User Support Team in IT Services were trained and undertook initial work
- Rollout started for Senior University Officers
- Uptake was slow because people were too busy for appointments
- Some early successes were noted



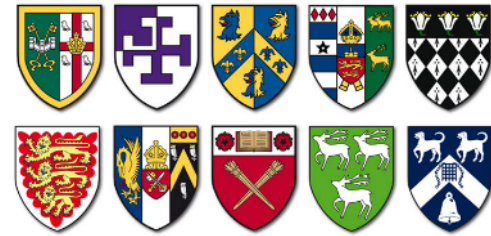
# More resource provided

- Project manager appointed WDE administrator and two technicians
- Speeded up rollout considerably on the back of UAS Windows 7 rollout
- “Clinics” provided for self-managed computers in IT Services and rest of UAS
- Many were able to self-install
- This phase finished now

# ITSS are crucial to WDE

- Devolved deploy and support model works best in Oxford University
  - You can reliably identify your users better than we can
- ITSS training and accreditation has been a great success
- Means that WDE is rolling out much wider than just UAS
- Accreditation is per ITSS not per ITSS affiliation
  - College ITSS can setup and support division-authorized person
- IT Services helpdesk trusts accredited ITSS with recovery tokens
- All units have been written to by Director of IT Risk management to encourage takeup

# What about College people?



- Bursars, Academic Administrators, Medical staff and more have confidential data
- College data leaks can damage University reputation too
- WDE for these people available to purchase via IT Services Shop



## Whole Disk Encryption for Colleges

£50.00

- 1 +

Add to Basket

### Description

This product is only for purchase by accredited College IT Staff and is solely for College Staff who have no departmental affiliation that would give them free use of the Whole Disk Encryption Service. This item entitles the user concerned to use the WDE service until 31 August 2016. After that time there will be no further support but the computer in question will remain encrypted so IT Staff should ensure there are adequate backups in case of loss of access via lost passphrase.





# Some issues

- Support for OSX 10.9 and Windows 8.1 was slow to come from Symantec
- Windows recovery doesn't work as booting from RAMdisk doesn't load WDE driver
- Can make a BartPE disk with WDE
- It appears to be impossible to upgrade a Mac's OS without decrypting first
  - This takes days
  - Backup/wipe/reinstall/restore may be better
- Lots listed
  - <https://wiki.it.ox.ac.uk/itss/WDE/Instructions>

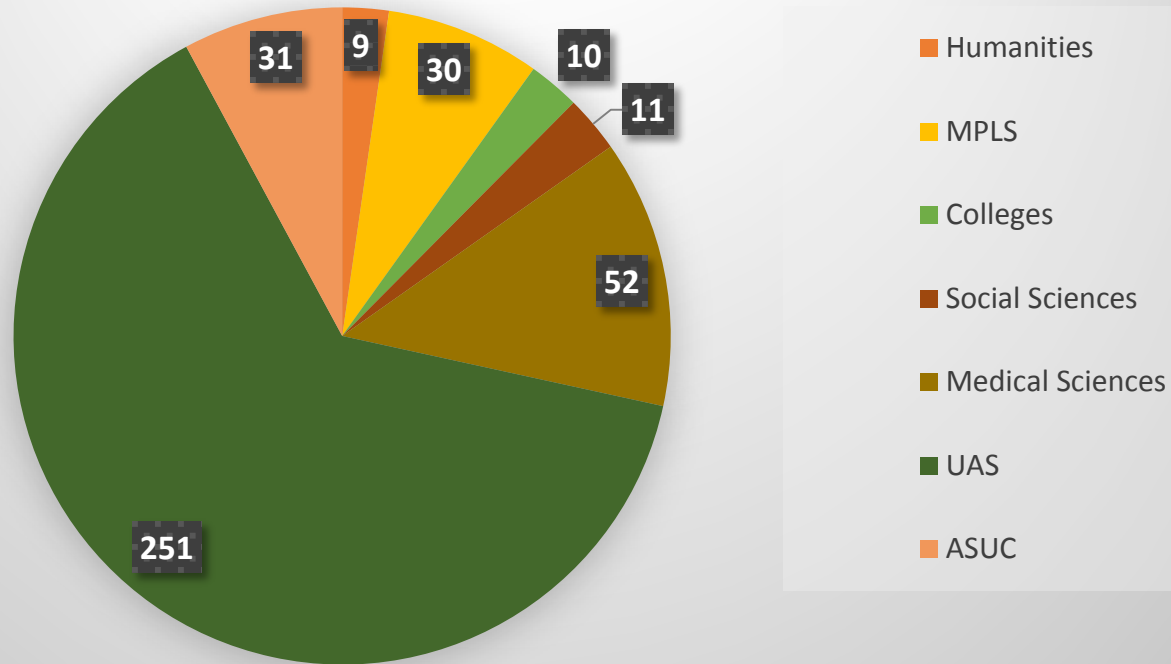
# Foreign travel needs careful consideration



- Some nations don't like encryption and can impose serious legal penalties
- In practice problems are rare
- Risks need to be properly assessed
  - See <http://www.it.ox.ac.uk/infosec/protectyourself/travel/>
- Good choice can be to take a clean laptop and only handle data through remote access
  - Nexus OWA
  - Citrix

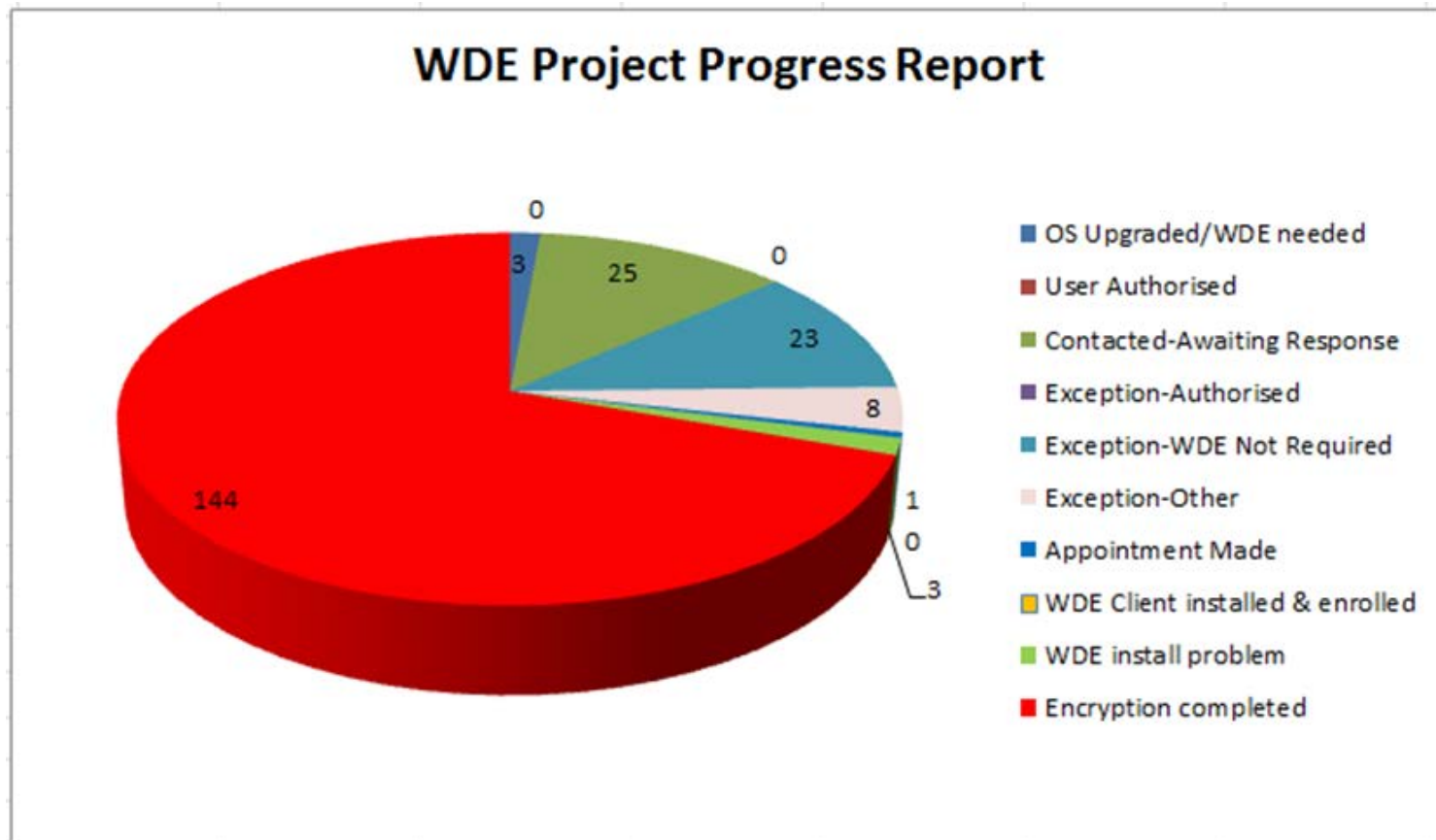
# WDE is spreading around the divisions

Encryptions by Division



# The project in numbers

- 104 ITSS successfully trained and accredited
- Only 8% of licences so far issued



# A quick note on TrueCrypt

- Was considered to be a good option
- **WARNING:** TrueCrypt is no longer developed/supported so newly discovered security flaws are unlikely to be fixed
- Development stopped in May 2014
- A good time to move to WDE!



**TrueCrypt**

# Alternatives to WDE

- Keep sensitive and/or personal data off laptops
  - Careful with Outlook cache etc.
  - Useful for foreign travel
- Use encrypted USBs



£45.00

- 1 +

Add to Basket

## Description

4GB Hardware Encrypted USB Stick

## Detailed Description

The iStorage datAshur<sup>®</sup> is the world's most secure, easy to use and affordable USB flash drive, employing PIN code access with military grade AES 256-bit hardware encryption. The datAshur is FIPS Security 140-2 Level 3 Certified (Certificate No. 1873) and incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN onto the on-board keypad before connecting the drive to the USB port. This drive does not require any software on the device it is plugged into and has the facility to set an administrator PIN that can be used to override the user PIN if it is lost. The device automatically locks when it is removed from a USB port.

These devices are branded Oxford University and IT Services and have the phone number of the IT Services shop etched on the drive itself for recovery in the case of loss. The IT Services Shop will record the serial number of each drive against the name of the person or unit that bought it. Note the cost is only £37.50 for University departments as the price here is quoted with 20% VAT.

# The future

- University will continue to monitor InfoSec requirements
- Current PGP licences run until 2016
- Price of college licences will drop month by month to recognise that
- More ITSS training and accreditation is scheduled
- More awareness activity should get more users coming forward for encryption
- Consider encryption as standard on new laptops

# A quick plug

- Systems and encryption are only half of the Information Security issue
- Social engineering and user error are big risks
- I strongly recommend (and UAS mandates) the Info Security Modules available FREE to all staff via weblearn  
It's coffee break stuff!
- <https://www.it.ox.ac.uk/infosec/module>





# Any questions?

- Thank you for coming to this workshop
  - I hope you have found it useful
  - I welcome feedback
- [tony.brett@it.ox.ac.uk](mailto:tony.brett@it.ox.ac.uk) @tonybrett
- WDE info for ITSS at <https://wiki.it.ox.ac.uk/itss/WDE/Instructions>
- WDE info for users and ITSS at <http://www.oucs.ox.ac.uk/wde/>