

PROSPECTS
hedd

VERIFICATION + AUTHENTICATION

 Department
for Education

Advice and guidance on degree fraud

A toolkit for employers

Contents

1.INTRODUCTION	Action against applicants.....6	Report to Action Fraud and the National Fraud Intelligence Bureau.....8
2.TYPES OF DEGREE FRAUD	Share false documents and fraud evidence.....6	Cifas and Amberhill.....8
Bogus universities and degree mills.....3	4.WHAT ACTION CAN BE TAKEN?	ENIC-NARIC and International.....9
Copycat websites.....4	Fraud legislation.....7	6.APPENDIX
Fake certificate sites.....5	Forgery legislation.....7	Tips for identifying bogus UK university websites, certificates and other documents.....10
Individuals.....5	Recognised degree awarding bodies.....7	UK Register of Learning Providers.....11
3.RECOMMENDATIONS FOR EMPLOYERS	Protection of the word 'university'.....7	Misinformation.....11
Formal policy on degree fraud.....6	'ac.uk' domains.....7	Examples of bogus providers masquerading as genuine UK universities.....11
Who to involve.....6	Higher education degree datacheck (HEDD).....7	Example template for a student consent form.....12
Information for applicants.....6	5.WHO CAN HELP?	
Making verification checks.....6	Department for education (DfE)/	
Action against current employees.....6	Prospects HEDD fraud service.....8	

1.INTRODUCTION

This toolkit has been developed for recruiters. It contains advice and guidance on degree fraud for HR departments. It has specific recommendations for putting preventative measures in place during recruitment, advising applicants better and for taking action once evidence of fraud is found. It also gives details of how to make verification checks with UK universities and overseas.

There is reported to be a growing number of instances of misrepresentation and forgery in the presentation of academic credentials. Until recently, little has been known about the scale and nature of degree fraud. In every survey covering the subject around one third of people admit to lying on their CV, with misrepresenting educational qualifications being the most common lie. A recent analysis of 5,500 CVs by the Risk Advisory Group (March 2016) found that 44% of CVs had discrepancies in education claims with 10% of those having false grades. This was an increase of 7% on the previous year. Prosecutions are rare, with fake

qualifications usually only coming to light as part of another investigation.

Managed by Prospects, Higher Education Degree Datacheck (HEDD) was launched six years ago with funding from the Higher Education Funding Council for England (HEFCE). It provides a degree verification service for applicants to employment or entry into postgraduate courses. It seeks to protect UK graduates, universities and employers from degree fraud.

In June 2015 the Department for Education (DfE) and careers expert, Prospects launched a new service to reduce higher education fraud in the UK.

The service was commissioned by DfE to proactively address issues concerning bogus institutions and the misuse of the word 'university' as well as to tackle the related area of degree fraud. It aims to crack down on bogus provision and fraudulent behaviour by increasing prosecutions through investigation and awareness-raising.

Research by HEDD found that only 20% of employers verify applicants' qualifications with the awarding body, relying instead on CVs or certificates and transcripts. Since its launch, HEDD has identified more than 230 bogus providers and websites selling fake degree certificates and processed more than 160,000 individual verification checks. 5% of the checks made through HEDD are based on false qualification claims and this is after consent has been given by the applicant for the check to be made.

Advice and guidance has also been published for universities and students and graduates.

Thanks go to the many agencies, employers, Higher Education providers, Government departments, professional associations and colleagues in law enforcement authorities who have contributed to the development of this toolkit.

Jayne Rowley, Chief executive,
Prospects June 2017

About Prospects

Prospects is the UK's leading provider of information, advice and opportunities to students and graduates. Prospects is the commercial trading subsidiary of the Higher Education Careers Services Unit (HECSU), a higher education agency and registered charity.

Graduate Prospects, Prospects House,
Booth Street East, Manchester M13 9EP, UK
t 0161 277 5200 e heddteam@prospects.ac.uk
www.prospects.ac.uk · www.hedd.ac.uk
www.heddblog.wordpress.com @HEDD_UK

Company Reg No.2626618 · Copyright 2017 © Graduate Prospects 2017

2. TYPES OF DEGREE FRAUD

Degree fraud refers to crimes committed in relation to higher education qualifications. It commonly falls under fraud, forgery, trade mark or copyright legislation. Details on the legislative measures can be found in the ‘What Action Can Be Taken?’ section.

There are three broad types of degree fraud: bogus universities and degree mills; fake certificate websites; and fraud committed by individuals. Advice on identifying fake websites and documents is covered in the Appendix.

Bogus universities and degree mills

Bogus universities and degree mills operate purely to make money – from enrolment fees, premium phone lines, course fees and ‘life experience degree’ awards – and in doing so provide a means for fraudsters to obtain

authentic-looking degrees and associated documentation from unaccredited institutions. This type of fraud is becoming more sophisticated, with credible websites and verification services often modelled on their

authentic counterparts – including the direct lifting of content and sections of material from genuine university websites. This is designed to back up fake documents and fool employers into believing a credential check has been made.

Case study

The International New York Times published a story in May 2015 following a long investigation into an alleged network of diploma mills and bogus websites controlled by Pakistani software company Axact. It’s an excellent example of the techniques used by degree mills to generate revenue.

<http://www.nytimes.com/2015/05/18/world/asia/fake-diplomas-real-cash-pakistani-company-axact-reaps-millions-columbiana-barkley.html>

This is degree fraud on a global scale with 370 websites cited by the New York Times as being part of the operation and individuals being duped out of multi-millions of dollars and pounds by unscrupulous and clever operators. The websites have names and details evoking the appearance of American or British universities and use stock photography or actors to create an authentic look.

After a raid at their Karachi office officials said hundreds of thousands of blank degree

forms, student cards and authentication documents were found.

Bogus universities also target genuine individuals looking for online or distance education, with coursework sent out for completion and submission, recommended reading lists – usually lifted from the online resources of legitimate academics and courses. These victims spend thousands of pounds for what is essentially a worthless qualification.

Case study

The target receives an email from an education recruitment agency saying that they are eligible for a major scholarship for a top UK online university, which covers 95% of the tuition fees.

Instead of £10,000, they can enrol on an MBA course at Rutland University in Leicester for just £699. They are urged to complete the application form with payment within the next 24 hours to secure the scholarship. Thinking they are getting an expensive education at a bargain price they complete the application form, pay the £699 and begin their online assessments.

One victim contacted HEDD with concerns about Rutland’s legitimacy.

‘Things are actually going well and I have been taking online assessments as part of the online course until recently, I was told

that I need to take a final assessment in order to participate with the “online convocation” and be able to receive my certificate and transcript of records... That made me feel suspicious since it was never mentioned before regarding additional fees when taking final assessment... I did the payment (another £250), although I was doubtful, and took the final examination. There was no online convocation that happened.’

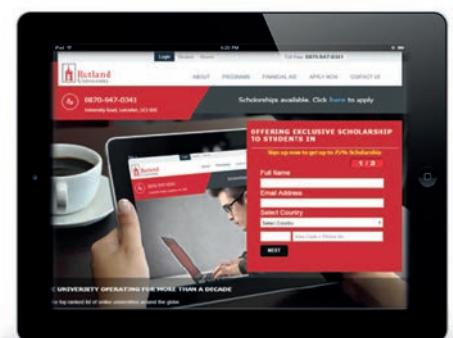
HEDD’s investigation found the following: Rutland University uses the address of a real UK University and names one of its professors as their President.

They claim to be accredited by the British Distance Learning Association – a fictitious body.

The phone number on their website doesn’t work, nor the online chat. All communications are by email.

HEDD has reported them to the authorities and the website has been shut down. Unfortunately the victim has almost certainly lost their money and doesn’t have a recognised UK degree.

There have been a number of bogus sites advertising scholarships lately – potentially all from the same degree mill running a number of fake websites.



2. TYPES OF DEGREE FRAUD

Copypat websites

Some bogus providers emulate genuine UK HE providers by setting up copypat websites using a real university's name, lifting information or images from the genuine site. They generate revenues from enrolment fees or premium phone

lines by duping applicants who believe it is the genuine university, but also allowing fraudsters to gain plausible, but fictitious credentials.

Degree certificates and transcripts are issued by the operator and the websites

offer verification services for employers to check their 'graduates'.

Examples of bogus providers masquerading as genuine UK universities can be found in the Appendix.

Case study

A degree mill was set up as the University of Wolverhampton (note the mis-spelling). The website used wording and images from genuine university websites, including the real University of Wolverhampton. Fraudsters present certificates and transcripts to employers as genuine. The transcript carries details of how to check its validity by going to the website.



At the top is a 'search profile' button. The student number from the transcript is entered and the student's details are confirmed on screen. The employer thinks they have verified the applicant.

HEDD investigated and the website was shut down. As is often the case, it reappeared several months later with its name changed to Warnswick University. This too has been investigated and shut down by HEDD.

2. TYPES OF DEGREE FRAUD

Fake certificate sites

There are a multitude of websites offering 'novelty' or 'replacement' degree certificates. These websites carry disclaimers about not using the documentation to make fraudulent misrepresentations in order to avoid prosecution. However they are breaching the copyright and trade marks of the universities whose certificates they are imitating. They often base their templates on real certificates. There are lots of images of real certificates innocently posted online by graduates on Twitter, on social media sites like Instagram and Facebook and lifted by fake certificate sites. These sites rely on having access to real

certificates in order for their fakes to pass muster with recruiters. None of us would upload a copy of our passport or driving licence, nor give out our bank details.

If not, they create a generic template and fraudsters provide the details of the institution, award, classification and their personal details.

They include crests and logos for the institution which are easily accessible online.

They use official-looking stamps allegedly from registries, notaries, embassies, consulates etc. to lend authenticity. They add holograms to give an impression of security.

More expensive services offer transcripts, letters

of verification and references to create a portfolio of credentials. With transcripts and references as well as a certificate, the employer is less likely to contact the awarding body for confirmation.

In addition to websites, operators also use online marketplaces like Ebay and Amazon to sell certificates, for as little as £7. Both Ebay and Amazon have terms and conditions that prevent fake certificates being sold via their websites and also have mechanisms to report sellers breaking the rules. However, some of the sellers have notched up hundreds of recorded transactions with satisfied customers leaving positive feedback about the quality of the products.

Case study

Over the summer large numbers of photo tweets of graduates appeared posing with their degree certificates at ceremonies around the UK. To celebrate their graduates' successes, these were frequently and innocently re-tweeted by their universities.

Once published and added to the gallery of Google images these photos give anyone looking to make fake degree certificates the current designs for many UK universities, which they can then duplicate – logo, crest, signatory,

stamps, holograms and forms of words.

HEDD contacted every university's social media team to advise them not to include certificates in their photo tweets and to advise their students not to do so either.

Case study

The degree fraud team at HEDD spotted a seller offering 'novelty' degree certificates from any UK university for £6.95 with free postage and Nectar Points on Ebay. Some mystery shopping seemed in order and HEDD purchased a number of certificates with different

qualifications from different universities. The subjects requested were clearly not for novelty purposes – one was for a Masters in Astrophysics and Space Technology (i.e. Rocket Science).

The certificates duly arrived, complete with crests, logos and holograms that could fool employers who often don't appreciate the security features built into genuine certificates. Helpfully the hard-backed envelopes in which the certificates arrived had the seller's name and return address on and the evidence was passed on to Trading Standards to investigate.

Individuals

Even if they don't buy fake documents from a third party, anyone who falsely creates a certificate or alters a genuine document from a real university – changing the name, subject, qualification or classification – and presents the documents as real is still committing fraud. These are hard to spot, as they are usually based on real certificates. The only way

to verify their authenticity is to check with the issuing institution or HEDD.

Making or supplying such documents is an offence in itself and constitutes fraud. Presenting this documentation as genuine in job applications constitutes fraud by false representation and can lead to prosecution resulting in prison sentences of up to ten years.

Case study

One woman made her own certificates and conned her way into two teaching jobs in Northampton and Devon and a role marking A level papers with an Exam Board. This was after using the fake certificates to get a place on a teaching course at a real University and obtaining a PGCE qualification. She was found out after applying for a teaching job in Torquay. The school were suspicious about her certificates and checked them with the awarding universities, where her deceit was revealed. This landed her 18 months in prison.

Case study

A bogus barrister received a 14 month (suspended) sentence and 200 hour community service order. Starting with a forged degree certificate in 2000 and forging other letters and credentials, she became a local government lawyer with several councils and rose to be the lead member for planning at a Borough Council. She was only found out when constituents began looking into her background after raising a number of complaints about her work identifying areas of land for development, not by her employers.

Case study

A man was jailed for four years after tricking people out of hundreds of thousands of pounds after posing as a doctor with a degree from the University of Cambridge and claiming to have led a research team at University College Hospital in London. He also claimed to have treated the Queen, Lord Sugar, Robbie Williams and went as far as to tell one 'patient' they had cancer. Even in court he persisted with his lies saying that he couldn't discuss his treatments as he was bound by the Official Secrets Act.

3. RECOMMENDATIONS FOR EMPLOYERS

Formal policy on degree fraud

The main recommendation is to develop and agree a formal HR policy on degree fraud. Once agreed it should be published and disseminated to departments and employees. Information for job applicants should be included on the website, on recruitment literature and on application forms.

Who to involve

As well as HR colleagues, in-house or external legal advisors should be included in any policy development, particularly with regard to any action the organisation may wish to take against individuals.

Information for applicants

- Include information about the fraud policy in recruitment literature and on the website
- Notify applicants that qualifications will be verified. If the candidates know checks will be made, this can be an effective deterrent.
- Include a verification consent form as part of the application process or include a check box for verification on the application form. A sample consent form can be found in the Appendix.
- Be clear about what action may be taken if fraud is discovered.

Making verification checks

- Include information in the policy on how credentials are to be verified.
- Do not rely on CVs. Always request certificates and/or transcripts – originals, not copies, where possible.
- Check with the Awarding Body. Details of how to verify applicants from all UK HE providers are published on HEDD and direct requests can be made through HEDD to over 40 universities. More are joining all the time.

- Use the ENIC NARIC network to check the recognised HE providers in other countries. See the 'ENIC NARIC and International' section.
- Verify official-looking or notary stamps – check with the signatory and ask if they verified the information on the original document or are just certifying a copy.
- If it's an award from a UK university that you are not familiar with, check the authenticity of the institution. Details of current and former UK degree awarding bodies can be found on the HEDD university look-up service. Over 230 known bogus providers are also listed there.

Action against current employees

If the organisation has not previously verified the qualifications of employees with the awarding bodies and is introducing a corporate policy to do so, it is essential to agree how current employees are to be handled.

If retrospective checks are to be made, decide how far back to go and what will be done if discrepancies are found. Policies need to be really clear here on how the employee will be dealt with. Consider the following scenarios:

One of the senior directors has an MBA, or so you believed from her CV when she applied some years ago. A verification check under your new policy shows that she began an MBA course, but did not complete it. She has a high external profile for the organisation.

A long serving employee with an exemplary work record and high level of skills and competence is revealed to have a 2:2, not a 2:1 as he claimed when he joined the organisation 10 years ago.

Consider whether to discipline them, terminate their employment, report them to the police, or share the information with databases

like CIFAS and Amberhill to prevent them committing fraud elsewhere. If you choose to ignore the deceit, this could set a dangerous precedent for future recruitment. Make this part of the published policy and assign responsibility.

Action against applicants

Too often employers reject candidates after lying on applications, but don't take action to report the fraud. One of the key reasons degree fraud thrives is because the perpetrators get away with it. If individuals clearly see that fraud doesn't pay, the temptation is reduced.

Share false documents and fraud evidence

Degree fraud is a borderless, global problem. In order for fraud to be investigated and reduced it is important to share information.

Keep records of fraud cases and any action taken.

Information can be passed on to HEDD using the fraud helpline on 0845 077 1968 or via the online reporting form www.hedd.ac.uk/contactUs.htm As well as the database of bogus providers, HEDD has a repository of fake certificates.

Share information and advice through professional employer networks like the Association of Graduate Recruiters (www.AGR.org.uk), Federation of Small Businesses, Chambers of Commerce.

Share with the national agencies like CIFAS and Amberhill, Action Fraud and the National Fraud Intelligence Bureau. Ensure that the policy on sharing has been notified on application or consent forms.

Case study

A solicitor has been lucky not to be struck off after an employer reported her to the Solicitors Regulation Authority (SRA). She had claimed to hold a 2:1 in a job application, when in fact she had a 2:2.

She believed that the 2:2 grade she had achieved was preventing her from getting permanent employment, despite getting high results in her Legal Practice Course and Professional Skills Course. When she applied for a position as a legal advisor, she lied about the grade.

The employer's strict recruitment process meant her deceit was

uncovered, even before she was interviewed, when they requested her original certificates. At that point she confessed – justifying her lie as a means to obtain an interview, after which she had intended to come clean.

The employer not only cancelled her interview, but reported the fraud to the SRA. They took action - suspended her from practising law for 18 months and fined her £3,000. The long term damage to her career could be far more costly. The case made the news and therefore a permanent home on the internet.

4. WHAT ACTION CAN BE TAKEN?

There is a range of legislative measures in respect of these matters, particularly on fraud, forgery, trade marks and copyright. The sections relevant to employers are outlined below.

Degree awarding powers, university title, ac.uk domains are strictly regulated and there are excellent sources of information and advice available.

Fraud legislation

There are a number of sections of the Fraud Act 2006 relevant to degree fraud.

Under the terms of Section 2 it is an offence to make a false representation with the intention of making a personal gain, causing a loss to someone else or exposing someone else to the risk of a loss.

A representation is false if it the person making it knows that it is, or might be untrue or misleading.

When someone lies on an application form or CV, presents a fake certificate or transcript or alters a genuine university document and presents the information as real they have committed fraud and can be prosecuted. It could result in prison sentences of up to ten years.

Forgery legislation

Under the terms of the Forgery and Counterfeiting Act 1981 a person is guilty of forgery if he makes 'a false instrument' with the intention that he or another shall use it to induce somebody to accept it as genuine. It is also an offence for a person to use such a false instrument with the intention of inducing somebody to accept it as genuine.

Recognised degree awarding bodies

The Department for Education (DfE) is responsible for maintaining lists of current recognised UK degree course providers. This comprises institutions who have their own degree awarding

powers (known as Recognised Bodies) as well as institutions who deliver degree courses that are awarded by a 'Recognised Body' through validated or franchised arrangements.

Under sections 214-216 of the Education Reform Act 1988, it is an offence for a body to award a UK degree or offer a UK degree course unless that body is already recognised and officially listed.

Protection of the word 'university'

The Companies House Act 2006 states that the approval of the Secretary of State for Business, Energy and Industrial Strategy (BEIS) is required for the name of a company or business to be registered if it includes a sensitive word or expression specified in regulations. The word 'University' is covered by this.

'ac.uk' domains

Organisations recognised as having Degree Awarding Powers in the UK are eligible to use an ac.uk domain. Legitimate HE Providers in the UK have the 'ac.uk' domain. There are strict eligibility guidelines and policies for the domain. Bogue websites sometimes acquire an '.ac' domain from the Ascension Islands for their websites to imitate genuine UK providers.

Higher Education Degree Datacheck (HEDD)

University look-up service

Like DfE, HEDD also maintains a database of UK recognised degree awarding bodies. In addition to the current HE providers, HEDD includes historical information on former recognised bodies, name changes, mergers etc. going back to 1990.

It includes dates and details of where the student records for current and former

HE providers are held and how to make a verification enquiry about current students and former graduates from those institutions.

Bogus providers

The look-up service also lists over 230 known bogus providers and unaccredited institutions claiming to offer UK degrees. This is updated regularly. It's important to distinguish between the completely bogus providers and alternative

providers which are perfectly legitimate places of study, but whose degrees are not recognised UK degrees. If they claim to award UK degrees, HEDD advises them to remove the misleading information from their websites. If they don't remove it, they are highlighted on HEDD as not being degree awarding bodies.

www.hedd.ac.uk/search_university_or_college.htm

5.WHO CAN HELP?

Department for Education (DfE)/Prospects HEDD fraud service

As stated earlier the Department for Education (DfE) and Prospects which runs the HEDD service launched a new initiative in June 2015 to reduce higher education fraud in the UK. Universities and Science Minister Jo Johnson announced the service at the Going Global conference.

The service was commissioned by DfE to proactively address issues concerning bogus institutions and the misuse of the word 'university' as well as to tackle the related area of degree fraud.

Bogus providers are targeted by HEDD. Perpetrators found to be masquerading online as genuine providers with degree awarding powers are added to the database of bogus institutions. HEDD

investigates who owns the websites and where they are hosted, liaises with Trading Standards and other enforcement bodies, including those overseas to prosecute and force closure.

A telephone helpline has been set up for advice about degree fraud or to report dubious organisations. Call 0845 077 1968. An online reporting form can be found here:

www.hedd.ac.uk/contactUs.htm

This toolkit has been developed as part of the service to support recruiters who find themselves victims of application fraud and assist them to take action if necessary.

Report to Action Fraud and the National Fraud Intelligence Bureau

Action Fraud

Action Fraud is the UK's national fraud and internet crime reporting centre providing a central point of contact for information about fraud and financially-motivated internet crime. Action Fraud refers all fraud crime cases and information on fraud to the National Fraud Intelligence Bureau (NFIB).

National Fraud Intelligence Bureau (NFIB)

NFIB is hosted by the City of London Police to combat fraud of all kinds and through its Cyber Prevention & Disruption Team helps to direct the UK's response against fraud. They work in partnership with law enforcement, and other partners

to combat or disrupt fraud. Not every report results in an investigation, but every report helps to build a clear picture of fraud within the UK and makes it more difficult for fraudsters to operate in the UK.

www.actionfraud.police.uk/report_fraud

Cifas and Amberhill

Cifas

Cifas is the UK's Fraud Prevention Service – a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime. It provides a database of confirmed fraud in the UK, enabling members to share confirmed fraud cases and cooperate to combat fraud.

The Cifas team works closely with UK law enforcement partners, including the City of London Police (National Fraud Intelligence Bureau), the National Crime Agency and the Metropolitan Police Service as well as collaborating with HEDD.

www.cifas.org.uk

Amberhill

Amberhill is part of the Metropolitan Police Service's strategy to tackle identity crime. The Amberhill database draws together data relating to false documents. This data is cross-checked against other databases to identify fraud and deception in both the public and private sectors. The data is available to public and private sector organisations where a data sharing agreement exists, and thus supports existing systems that organisations have in place to tackle fraud. HEDD is working with Amberhill to share evidence of degree fraud and fake degree certificates and recruiters are encouraged to do the same. As stated earlier

presenting fake credentials is a criminal offence, so permission from the applicant to report and pass on false documents is not strictly required, although it could help fraud prevention if recruiters state that their policy is to share evidence with law enforcement agencies.



5.WHO CAN HELP?

ENIC-NARIC and international

When recruiting graduates from overseas it's equally important to verify academic credentials. Firstly to establish that the degrees and diplomas are equivalent to UK higher education qualifications

and that the institutions are recognised degree awarding bodies in their country. Secondly to ensure that the individuals have obtained the qualifications they claim.

ENIC Network (European Network of Information Centres)

The Council of Europe and UNESCO established the European Network of National Information Centres on academic recognition and mobility (ENIC Network) to develop policy and practice for the recognition of qualifications. They provide information on the education systems in their own and other countries, including the recognition of foreign diplomas, degrees and other qualifications.

NARIC Network (National Academic Recognition Information Centres in the European Union)

The NARIC network aims at improving academic recognition of diplomas and periods of study in the Member States of the European Union (EU) countries, the European Economic Area (EEA) countries and Turkey.

UK NARIC is the National Agency responsible for providing information, advice and opinion on vocational, academic and professional skills and qualifications from all over the world. UK NARIC provides vital support to universities, colleges and employers with international recruitment and the processing of international applications for work or study.

www.naric.org.uk

ENIC-NARIC website

This site, a joint initiative of the European Commission, the Council of Europe and UNESCO, has been created primarily as a tool to assist the ENIC-NARIC Networks. There is information on recognised HE providers for each country, qualifications frameworks, qualification equivalence, education systems, country profiles etc. There is also information on unaccredited institutions, degree mills and fraud. Colleagues within the ENIC-NARIC networks exchange information to prevent fraud and identify the perpetrators. It's an excellent source of information on Europe and beyond.

www.enic-naric.net

Groningen Declaration Network

The Groningen Declaration Network (GDN) is an association of organisations in countries around the world dedicated to improving global student data mobility.

It consists largely of national agencies responsible for verifying student and graduate credentials on behalf of their countries. In many cases these are comprehensive, mandatory databases containing details of all graduates from recognised higher education providers. For the UK, HEDD is the national service, but it is

not currently mandatory for UK HE providers to be part of the HEDD system. In other countries e.g. China, South Africa, Mexico, Netherlands it is the remit of the Ministries of Education. A list of GDN members can be found here:

www.groningendeclaration.org/

HEDD is working with colleagues in the Network to exchange information, to assist recruiters to make credential checks for overseas applicants and to use their local knowledge to deal with bogus providers based in their countries and not subject to UK Law.

Case study

There have been a number of websites selling fake certificates and transcripts from up to 60 UK universities operating out of China. One such site was reported by one of the universities and investigated by the BBC. HEDD passed the information to GDN colleagues in the Chinese Ministry of Education who reported it to their

cyber crime unit, committed to shutting down fraudulent sites. The website has been taken down as a result. This is an effective route to deal with overseas operators.

In addition, the agency has published a list of bogus providers passing themselves off as Chinese universities and shared the data with the Network.



6.APPENDIX

Tips for identifying bogus UK university websites, certificates and other documents.

What to look for:

- Websites – what is the domain suffix?
Genuine UK degree awarding bodies have .ac.uk domains which are carefully restricted. Some bogus sites use an Ascension Islands domain to give them a .ac address to mimic genuine sites.
- Accreditation bodies – fake providers use fake accreditation bodies to look authentic – check these too. N.B. sometimes it's the same operators. They will answer designated phone numbers as the accreditation body, confirming the fake provider.
- Check the university is on the list of current Recognised and Listed Bodies on the UK Government website
www.gov.uk/check-a-university-is-officially-recognised/recognised-bodies
- Check the provider on HEDD (www.HEDD.ac.uk) which has the current Government list, but also has historical data on universities covering mergers, name changes etc. and known bogus universities.
- Check the HEFCE Register which lists HE providers regulated in England.
www.hefce.ac.uk/reg/register/
- Check the OFQUAL Register which contains details of Recognised Awarding Organisations and Regulated Qualifications in England (Ofqual), Wales (Welsh Government) and Northern Ireland (Ofqual for vocational qualifications and CCEA Accreditation for all other qualifications).
www.register.ofqual.gov.uk/
- Check the list of providers with a Tier 4 licence to sponsor international students on Gov.uk
www.gov.uk/government/uploads/system/uploads/attachment_data/file/498142/2016-02-05_Tier_4_Register_of_Sponsors.pdf
- Non UK English spelling – honors, program, labor, organization, endeavors
- Inconsistent information. Bogus websites often cut and paste information from different sites. The fake Wolverhampton site refers to central England, London and Dublin.
- Non-functioning links. Some pages and links may be under construction or broken.
- Non UK references. References like the 'Dean's List', 'Matriculation Dates', 'Fall Semester' - US references that wouldn't be used by UK providers.
- Incorrect spelling and grammar – examples HEDD has found include studnets, gradaute, regestry, scholarship.
- Order of title – which way does the university refer to itself? – The University of Manchester (real), or 'Manchester University' (fake). This can be easily checked on HEDD.ac.uk
- Use of Latin. Expressions like 'cum laude' are popular with US universities but UK HEIs use 'with honours'. It has not been practice for UK providers to issue degree certificates in Latin for at least 10 years. Contemporary certificates are in English. Latin versions are occasionally issued as mementos, but are supplementary to the English version.
- Gothic script – very popular with fake universities – rarely if ever used by real UK HE providers.
- Signatories and officials – is it the correct Registrar's name, or Vice Chancellor's? Was it correct at the time of study? This is easy to check online.
- Locations – use Google Maps – use Streetview to take a look – does the address exist? Does it look like a university building?
- Addresses – is it a PO Box or mailing house? This can indicate a bogus website.
- Phone numbers – is it a real number? Is it a UK number? N.B. premium rate numbers are often used by fake universities, going to recorded messages, but charging the caller extortionate amounts.
- Written references – research the referee online and contact them if they check out. Don't just trust a letter, which could be forged.
- Stamps – it's very easy to get a stamp made up e.g. 'certified as a true copy' and include a forged signature of a notary or solicitor.
- Notaries – even if it carries a genuine notary signature or stamp, this doesn't necessarily authenticate the certificate. Notaries attest to sight of an original document, not whether that document or the information is verified.
- Seals, crests and holograms – these are easy to create – check the crest with the real university website – does it match?
- See the original, not copies, nor scanned PDFs – photoshopping is common.
- Name – is it close to a real university name 'University of Wolverhamton', 'Redding University'?
- Evidence of cutting and pasting on documents – is everything straight, same fonts, no visible lines? This could indicate an altered document.



6. APPENDIX

UK Register of Learning Providers

The UK Register of Learning Providers (UKRLP) is owned by the Skills Funding Agency and its database is a register of the legal entity details of learning providers in the UK. More than 30,000 learning providers are registered and all legitimate degree awarding bodies will appear there.

As stated on the UKRLP website any organisation or establishment, whether public,

voluntary, charitable or private that provides learning, advice or guidance from any UK location either directly or via sub-contracted providers can register, provided it is a legal entity in the UK.

Registered organisations are issued with a UK Provider Reference Number (UKPRN) and this can be verified on the UKRLP website.

However, it is not an accreditation scheme

and does not carry out quality checks on the learning provision of organisations on its register. That is not its purpose. Organisations on the register are strictly forbidden to use any references to the UKRLP which may imply accreditation, endorsement or assurance of its provision. Holding a UKPRN does not provide evidence of any endorsement by UKRLP.

www.ukrlp.co.uk

Misinformation

There are a number of providers delivering qualifications that may be broadly categorised as “higher education” even though they do not lead to the award of a UK degree. This may be because the qualification is an award delivered by the UK campus of an institution that is based overseas, or because the qualification is

below degree level, e.g. a diploma or certificate. These complexities can give rise to confusion among potential students and some unscrupulous providers exploit this by not giving clear information on their websites about their status, nor the status of the courses and qualifications they offer.

DfE and HEDD receive enquiries from students who believe they are following courses leading to a recognised UK degree, due to misinformation from providers. This is particularly common for distance-learning or online provision.

Always check the status of the provider applicants have studied with.

Examples of bogus providers masquerading as genuine UK universities

These are just some of the known bogus UK universities. Most if not all of the websites for these have now been shut down, but fake certificates are still in circulation, so the details are listed on the university look-up service on HEDD.ac.uk to help employers.

- Ashbourne University
- Bedford University
- Berkshire University
- Blackpool University
- Bridgewater University
- Cambridgeshire University
- Canterbury University
- Chelsea University
- Cheshire University
- University of Coventry (the genuine institution is ‘Coventry University’)
- University of Devon
- Devonshire University
- Doncaster University
- Dorchester University
- Dover University
- University of England at Oxford
- Glastonbury University
- Grantchester University
- Greater Manchester University
- Halifax University
- University of Hampshire
- Hampstead University
- Heriots University
- Kensington University
- Knightsbridge University
- Liverpool Metropolitan University
- London University College
- Manchester University (The genuine institution is ‘University of Manchester’)
- Manchester Open University
- Marylebone University
- University of New Castle (the genuine institution is ‘University of Newcastle’)
- North West London University
- Oxford International University
- Preston University
- Redding University
- Rutland University
- Shaftesbury University
- Somerset University
- St Georges University
- Stafford University
- Surrey University (the genuine institution is ‘University of Surrey’)
- University of Sussex at Brantridge
- Thames University
- Wakefield International University
- University of Wexford
- Weybridge University
- Wiltshire University
- University of Winchester (the genuine institution is University of Winchester’)
- University of Wolverhampton (the genuine institution is University of Wolverhampton’)

6.APPENDIX

Example template for a student consent form

[Organisation Logo]

Verification request consent form

By completing this form, you are giving permission to [Organisation Name] to submit a verification request to the education institution that awarded your degree. Higher education providers will not accept verification requests without this form.

Please be aware that false information may be shared with law enforcement and related third parties for the purposes of fraud prevention.

First Name(s)
Last Name (at time of studying)
Date of Birth
Higher Education Provider/University
Qualification type (BA, MA, PhD etc.)
Title of Award (Course name)
Year of Award
Classification (1st, 2:1, 2:2 etc.)

I authorise [Organisation Name] to receive information relating to my education with the higher education provider listed above and to verify the accuracy of all information received.

I authorise the higher education institution listed above to release information about my academic history and qualifications to all persons, firms, agencies or companies which may request this information in connection with my application for employment with [Organisation Name].

In authorising release of this information, I hereby release the higher education provider listed above and all individuals associated with that provider from any and all liability that may result from providing this information to [Organisation Name]. This authorisation will be valid for three (3) months from the date of my signature below.

I understand that information that proves to be false may be shared with law enforcement and related third parties for the purposes of fraud prevention.

Candidate full name
Candidate signature
Date (DD/MM/YYYY)