PROSPECTS hedd
VERIFICATION + AUTHENTICATION

Department for Education

Advice and guidance on degree fraud

A toolkit for higher education providers

PROSPECTS hedd

Department for Education

Contents

1.INTRODUCTION

This toolkit has been developed for Higher Education Providers. It contains advice and guidance on degree fraud for registries and student services; admissions and compliance teams; human resources; marketing and brand managers and legal teams. It has specific recommendations for putting preventative measures in place at institutions; advising students better; developing monitoring policies; recruitment and admissions policies and for taking action once evidence of fraud is found.

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 know 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. 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 job applications or entry into postgraduate courses. It seeks to protect UK graduates, universities and employers from degree fraud. HEDD is part of a suite of activities under the University Modernisation Fund (UMF), a HEFCE fund that aims to help universities and colleges deliver better efficiency and value for money through the development of shared services.

In June 2015 the Department for Education (DfE) and 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 processed more than 160,000 individual verification checks. Five per cent of the checks made through HEDD are based on false qualification claims and this is after consent has been given for the check to be made.

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

Thanks go to the many agencies, 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

HIGHER EDUCATION FUNDING COUNCIL FOR ENGLAND hefce

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.

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:

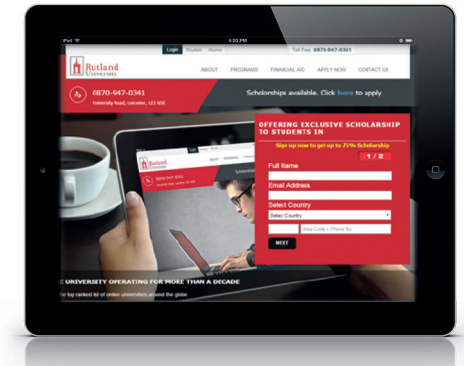
Rutland University uses the address of a real UK University and names one of its professors as their President.

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.



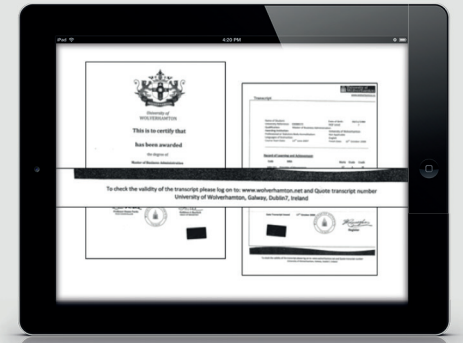
Copycat websites

Some bogus providers emulate genuine UK HE providers by setting up copycat 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'.

Case study

A degree mill was set up as the University of Wolverhamton (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.

Fake certificate sites

There are a multitude of websites offering 'novelty' or 'replacement' degree certificates for as little as £7. 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.

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.

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 purportedly 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. HEDD has done mystery shopping tests and purchased certificates that could fool employers who often don't appreciate the security features built into genuine certificates.

The websites carry disclaimers about offering 'novelty' or 'replacement' certificates which should not be presented as genuine credentials to protect themselves, but they are breaching the trade marks of genuine universities and can be shut down and prosecuted.

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 HIGHER EDUCATION PROVIDERS

Formal policy on degree fraud

Carrying out the research for this toolkit, it emerged that many universities don't have a formal policy on degree fraud although ad hoc or discretionary practices were in place. There is published information on academic fraud, but not qualification fraud. HEDD spoke to colleagues in registries, legal departments and marketing about their institution's policies. A small number said there was a policy in place but weren't aware of published information or what the policy was.

The main recommendation is to develop and agree a formal policy on degree fraud. Once agreed it should be published and issued to departments. Information for students should be included on the website, in the student handbook or upon registration.

Information relevant to third parties should be published on the website or in written documentation as appropriate, including details of how to make a verification enquiry about a former student or graduate.

Who should be involved

Degree fraud is an issue for a number of departments, but not the responsibility of a single area. Marketing, admissions, legal, registry and human resources all have a stake in managing fraud in this area and should be involved in developing and shaping internal policy.

Marketing are responsible for managing the brand presence and reputation for the HE provider. Copycat websites, breaches of trade marks and copyright rights normally fall under this area.

Admissions and compliance are responsible for recruitment and enrolment of students and university staff. Candidate verification and recognition of qualification equivalence as well as identifying application fraud falls into this area.

Human resources are responsible for recruitment of employees for the HE provider and the same verification policies should be in place as for student recruitment.

Careers and employability services are central to advising students and graduates about progression from university, making applications and CVs.

Things to cover in a degree fraud policy

Recruitment and admissions

- 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.
- Request certificates and documentation – original certificates 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 or NARIC networks to check the recognised HE providers in other countries.
- 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.
- Check on HEDD university look-up service. Over 230 known bogus providers are listed there.
- Notify applicants that they risk their place being withdrawn either prior to entry or after enrolment if it is found they lied about their qualifications or provided false evidence of their supposed qualifications.
- Share information on fraud. Let applicants know in advance that fraud is not tolerated and information will be passed on. Include details on the application form and on the consent form as part of the terms and conditions of applying. 'Information may be shared with law enforcement and related third parties for the purposes of fraud prevention.'

Action against individuals and former students

Decide what action to take in the case of former students inflating grades, changing subjects, tampering with certificates, producing fake letters of verification, claiming degrees they did not complete. Options could include revoking degrees, reducing grades, suspension for a fixed period.

Decide what action to take against current students where after enrolment it is found that they lied about their qualifications upon application.

Decide what action to take against individuals with no former connection to the university.

In all cases consider whether to report them to the police, or share the information with databases like CIFAS and Amberhill to prevent them committing fraud elsewhere.

Make this part of the published policy and notify staff, particularly in registries and admissions. Agree an internal policy and assign responsibility.

A suggested template for a cease and desist letter to an individual can be found in the Appendix under Examples and Templates.

Action against websites

Monitor the institution's brand online including images. This can often uncover evidence of copycat websites and sites selling fake certificates. Agree an internal process and assign responsibility.

Information on dealing with copyright and trade mark infringements and who can help is covered in later in the toolkit. Options include civil and criminal action.

A template for a cease and desist letter to a copycat website can be found in the Appendix.

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, via the online reporting form *www.hedd.ac.uk/contactUs.htm* or through the HEDD Jiscmail group HEDD@Jiscmail.ac.uk As well as the database of bogus providers, HEDD has a repository of fake certificates.

Share information and advice through professional networks within the HE sector e.g. the Student Records Officers Conference; Academic Registrars Council; Association of University Administrators; Universities Human Resources; Association of Legal Practitioners; Jiscmail groups and so on.

Share with the national agencies like CIFAS and Amberhill, Action Fraud and the National Fraud Intelligence Bureau as detailed in the previous sections. If the information concerns individuals ensure that the policy on sharing has been notified on application or consent forms e.g. 'Information may be shared with law enforcement and related third parties for the purposes of fraud prevention'.

Issue advice to students and graduates

HEDD research with students and graduates found that only 20% know that it is illegal to lie about qualifications. There are a number of ways to advise students about the consequences of fraud and about the university policy on dealing with fraud.

The HEDD website has advice for students and graduates:

https://www.hedd.ac.uk/aboutHedd.htm

Cifas has a leaflet entitled 'Don't Finish Your Career Before It Starts' which can be linked to or downloaded from their website. They will also provide printed copies upon request.

www.cifas.org.uk/research_and_reports

Include information on degree fraud and university policy in the student handbook or on registration to raise awareness.

Include a statement about sharing fraud information with third parties on the student collection notice e.g. 'Information may be shared with law enforcement and related third parties for the purposes of fraud prevention'.

Advise students not to post pictures of their degree certificates on social media or anywhere online. They should be treated as personal and private documents like passports, birth certificates or bank details. There is a risk of identity theft as well as giving fake certificate sites access to current degree certificates to copy.

Issue guidance with printed certificates reminding graduates that degree fraud is an offence and that the documents must not be tampered with or altered in any way. A simple notice is a quick win and can be easily implemented.

Remind students that replacement certificates can only be obtained from the university and that under no circumstances should they attempt to recreate certificates themselves, nor purchase one from so-called 'replacement certificate' websites. Give details of the process for ordering a replacement.

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 HE providers 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 and forgery legislation

Fraud

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 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.

www.legislation.gov.uk/ukpga/2006/35/section/2

Under the terms of Section 7 it is an offence to make or supply articles for use in frauds.

When someone makes, adapts, supplies or offers to supply a document knowing that it is designed or adapted for use for fraud they can be prosecuted. This could include websites producing fake degree certificates for sale or where a certificate is amended to, for example, enhance the individual's degree classification. Again, the maximum sentence is ten years.

www.legislation.gov.uk/ukpga/2006/35/section/7

Forgery

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.

www.legislation.gov.uk/ukpga/1981/45

Trade mark legislation

Universities register themselves as proprietors of trade marks relating to their names and device marks – usually in class 41, amongst others for services including teaching services provided by a university; undergraduate and postgraduate courses; professional training; educational services and paid educational services.

Using the name of a university with registered trade marks in domain names; posing as that university; using that university's device marks or words in documentation such as certificates is contrary to section 10(1) of the Trade Marks Act 1994 and Article 9(1)(a) of the Community Trade Mark Regulation (207/2009/EC).

As a result of using those names or devices, there is likelihood of consumer confusion and of association with the trade marks. This is an infringement of section 10(2) of the Trade Marks Act 1994 and Article 9(1)(b) of the Community Trade Mark Regulation.

www.legislation.gov.uk/ukpga/1994/26/contents

Copyright legislation

Higher Education Providers usually include copyright notices on their websites.

Sample Copyright Notice
(c) 2016, [UNIVERSITY NAME] all rights reserved. Material published by [UNIVERSITY NAME] on these web pages is copyright [UNIVERSITY NAME] and may not be reproduced without permission. Copyright exists in all other original material published on the internet by staff or students of [UNIVERSITY NAME] and may belong to the author or to [UNIVERSITY NAME] depending on the circumstances of publication.

Copycat or bogus websites often use material including images from real universities' websites which is an infringement of the copyright owner's rights under the Copyright, Designs and Patents Act 1988. The Act can be found here:

www.legislation.gov.uk/ukpga/1988/48/section/1

Section 16 of the Act sets out the rights of the owners of the copyright and can be found here:

www.legislation.gov.uk/ukpga/1988/48/section/16

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. DfE has no direct enforcement role (this being the responsibility of Trading Standards Departments). DfE's role is to advise the public about legitimate degree providers and to liaise with the enforcement authorities where appropriate where bogus degree providers appear to be operating in the UK.

www.legislation.gov.uk/ukpga/1988/40/section/214 – unrecognised degrees

www.legislation.gov.uk/ukpga/1988/40/section/215 – enforcement

www.legislation.gov.uk/ukpga/1988/40/section/216 – Identification of bodies granting or providing courses for recognised awards

Protection of the word 'university'

The Companies 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.

If the website claims to be a registered company using the word 'University' without being a recognised degree awarding body it can be reported to Companies House:

www.gov.uk/government/publications/reporting-fraud-about-a-company-to-companies-house/reporting-fraud-to-companies-house

'ac.uk' domains

Jisc has been responsible for the administration and registration of domain names under 'ac.uk' since 1996. Full information relating to the 'ac.uk' domain can be found at:

www.Jisc.ac.uk/domain-registry

There are strict eligibility guidelines and policies for the domain which can be found here:

https://community.jisc.ac.uk/library/janet-services-documentation/eligibility-policy

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. As mentioned earlier, bogus 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 more than 230 known bogus providers and institutions claiming to offer UK degrees that do not have degree awarding powers. This is updated regularly.

www.hedd.ac.uk/search_university_or_college.htm

A growing number of HE Providers accept verification requests from third parties directly through the HEDD service, which already covers over a third of UK graduates. Since HEDD launched four years ago, awareness of the risks of degree fraud is increasing and employers are becoming more vigilant. Ninety thousand verification checks have been made through the candidate verification service, which is growing all the time. This has enabled statistics and information to be gathered and give the first national picture of degree fraud for the UK.

5.WHO CAN HELP?

Department for Education (DfE)/Prospects HEDD service

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 genuine UK HE providers who find themselves victims of degree fraud and assist them to take action if necessary. Further advice is available from Prospects depending on the circumstances of the situation. An awareness campaign will provide clearer guidance on the surrounding issues to HE providers, employers, students and graduates.

Report to Trading Standards

Trading Standards services are delivered by local authorities.

England, Wales and Scotland

Call the Citizens Advice consumer helpline to report an organisation to Trading Standards. The consumer helpline will assess the problem and pass it on to Trading Standards if it's appropriate.

Telephone: 03454 04 05 06
Textphone: 18001 03454 04 05 06
Telephone a Welsh-speaking adviser: 03454 04 05 05
Textphone a Welsh-speaking adviser: 18001 03454 04 05 05

www.citizensadvice.org.uk/consumer/get-more-help/report-to-trading-standards/

Northern Ireland

Contact Consumerline to report an organisation to Trading Standards.

Telephone: 0300 123 6262

www.nidirect.gov.uk/contact-consumerline-to-make-a-complaint-or-ask-for-advice

The National Trading Standards eCrime Team (NTSeCT)

NTSeCT been set up by the National Trading Standards Board and by BEIS to investigate national online scams and fraud as well as support local and regional trading standards officers with their own e-crime investigations.

www.tradingstandardsecrime.org.uk/

Trading Standards may pass information on to other bodies with the power to take action against the organisation reported, including the police. If there is a prosecution it may require the giving of evidence in court.

It is worth noting that Trading Standards does not have to prosecute, even when it is clear that a criminal offence has been committed. They can choose to take no action or give the organisation a warning.

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).

www.actionfraud.police.uk/report_fraud

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.

The NFIB has the power to suspend or shut down website domains and/or telephone/email accounts. Please complete an NFIB Suspension Request Form which is available upon request from HEDD by emailing HEDDhelp@prospects.ac.uk or NFIB via NFIB-disruptions@cityoflondon.police.uk

Jisc Janet-CSIRT Security Team

Janet-CSIRT is the Computer Security Incident Response Team for Janet, the UK's education and research network. There is advice for HE providers on their website about what can be done in the case of website infringements, or they can be contacted directly. They also have a good relationship with the Ascension Islands' '.ac' registry NIC.AC which is based in the UK and has helped Janet shut down fraudulent sites.

https://community.jisc.ac.uk/library/janet-services-documentation/fake-colleges

Take direct action

There are options to take direct action. Abuse of copyright or trade marks and unlawful activity can be reported to hosting services, phone operators, website domain registries. They have policies in place to prevent abuse of their services and they have the right to suspend, block or remove services.

Check the websites of the relevant domain hosting service, phone operator etc. for their reporting mechanisms – usually online or by phone. A good place to start is 'whois' lookup services available via search engines which will give information about the domain owners, assignees, dates and addresses. Increasingly domain registrars offer private registrations (also known as domain privacy) by which the contact information of the registrar is shown instead of the customer. Personal information is collected by these registrars and they may release the information following a phone or written request reporting abuse.

'Cease and desist' letters are frequently used in disputes concerning intellectual property, or copyright and trade mark infringement. By informing the third party of the rights of the holders of the trade mark or copyright and signaling that those rights will be enforced, this can resolve the issue without escalating to Trading Standards or Action Fraud.

Jisc Janet-CSIRT have Template Notice and Take Down Policy and Procedures advice regarding the management of content on websites and the cease and desist template can easily be adapted for external use. See Examples and Templates Section for a suggested template.

Institutions should seek independent legal advice if they are concerned as to their position, particularly in light of the potential reputation ramifications of degree fraud for a HE provider.

http:/www.jisc.ac.uk/media/documents/themes/content/sca/templatenoticetakedown.pdf

Cifas and Amberhill

Cifas

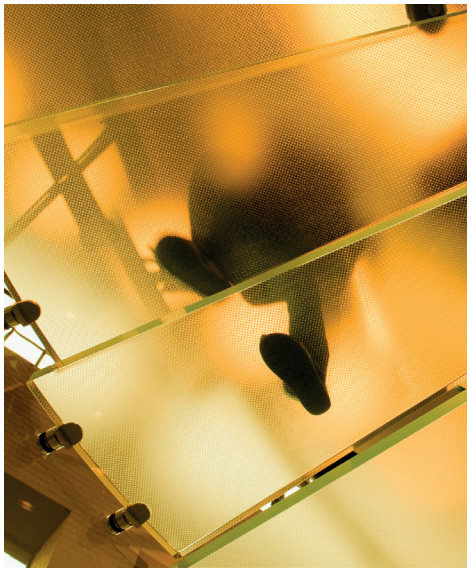
Cifas is the UK's Fraud Prevention Service – a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime. It provides a database of confirmed fraud in the UK, enabling members to share confirmed fraud cases and cooperate to combat fraud.

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. Data sharing agreements will have to be in place.



ENIC-NARIC and International

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. Signatories to the declaration commit to improving international student data exchange and seek to link with fellow signatories to facilitate student 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 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 Wolverhamton 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, scholorship.
- 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.

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 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.

Example template for a cease and desist letter to an individual

This example is for an individual with no connection to the HE Provider. When dealing with fraud by former students, the letter would have to be adapted to fit with the policy of the provider in regards to action, and addressing the particular circumstance of the fraud, e.g. tampering with a certificate, inflating grades on an application.

Insert logo) (Insert address)

Dear,

I am writing on behalf of ("**University**") [[in relation to the attached documents [**where possible it is always helpful to attach the documents**]] OR [as it has come to our attention you are relying on documents] which purport to be from the University [including a degree certificate and academic transcript showing that you graduated from the University in [insert]][("Document/s").

Our records show that you are not, and have not, been a student at the University and, as such, have not been awarded the qualification/s referred to in the **Document/s**.

In presenting the Document/s [and purporting to a third party that you have a qualification from the University], you have fraudulently used the University's name without consent and stated that you have qualifications from the University, when you do not.

The University takes its reputation, and academic integrity, extremely seriously and it is clearly unacceptable that you have presented Document/s which purport to be from the University and which purport to show that you have a qualification from the University when you do not.

The University does, and will, not tolerate fraudulent behaviour of the nature outlined above. Accordingly, the University requires you immediately to cease providing the Document/s to any third party and to confirm in writing to the University (addressed to me) by [insert date] that:

- you will not provide the Document/s to any third party in the future;
- where you have provided the Document/s to a third party, you will write to such third party, with a copy to me, to state that the Document/s are fake and must not be relied upon;
- you have destroyed any and all copies of the Document/s and requested any third parties who have received it to destroy their copies (in this context, "destroy" includes deleting any electronic copies of the Reference and shredding any paper copies of it); and
- you will not write and/or submit any other Document/s, or other information, purporting to be from the University and/or its employees.

Further action

Please note that, in the absence of satisfactory action by you in relation to the above, the University will have no option other than to consider taking further action in respect of this matter, including pursuing you for fraud. In the meantime, the University reserves all of its rights.

I look forward to hearing from you as above.

Signed: _____

This template has been adapted from a template Cease and Desist letter developed by the University of Manchester and made available with their kind permission.

Example template for a cease and desist letter to a copycat website

It is recommended that the HE provider's legal team lead or be closely involved in any direct action. This is a suggested format for a cease and desist letter which can be adapted depending on circumstances.

To: XXX (+ email address)
From: [Name, address, telephone number and email address of complainant.
Reference: [Title and unique identifier to which complaint refers] [subject of complaint].

1. Infringement of copyright/author's rights/related rights

a) The following material is protected by intellectual property and copyright law (Copyright, Designs and Patents Act 1988).

i) Describe the protected material in as much detail as possible so that the specific content, edition and format may be readily identified and indicate the category for protection under copyright law (e.g. original literary, dramatic or musical work, software). Specify exactly the extent of use, e.g. by quoting text that has been reproduced] (The Protected Material).

b) I/we own or am/are authorised to represent the owner of intellectual property rights in the protected material.

c) I/we hereby give notice of unauthorised use by reason of reproduction and/or making available the protected material.

2. Infringement of Trade Marks

a) Describe the trade marks held by the complainant (e.g University Name, device registered as "Trade Mark") and indicate the category/ies under which the marks are registered (e.g. class 41 teaching services provided by a university; undergraduate and postgraduate courses; professional training; educational services and paid educational services).

b) Using [Trade Mark] in domain names; posing as [Trade Mark]; using [Trade Mark owner]'s device marks or words in documentation such as certificates is contrary to section 10(1) of the Trade Marks Act 1994 and Article 9(1)(a) of the Community Trade Mark Regulation (207/2009/EC).

c) As a result of using those names or devices, there is likelihood of consumer confusion and of association with the Trade Marks. This is an infringement of section 10(2) of the Trade Marks Act 1994 and Article 9(1)(b) of the Community Trade Mark Regulation.

3. I/we hereby request, with reference to the subject of this complaint, you/your organisation:

a) Remove it from the website; and

b) Cease further use of the material; and

c) Withdraw from circulation any materials that include it.

4. I/we request that you notify me/us when you have complied with my/our request in section 3 above.

5. I/we attach/direct you to the following additional information which supports the complaint: [proof of ownership, etc]

6. In relation to my/our complaint, I/we also inform you [any other relevant information including other steps taken to protect my/our rights].

7. The information contained in this notice is accurate and I/we believe, with good faith, that the publication, distribution and reproduction of the material described in section 1 and 2 is not authorised by the rightsholder, the rightsholder's agent or the law and/or infringes the law as described in section 1/2 above.

8. This notice is given to you without prejudice to any other communication or correspondence relating to the protected rights or any other right.

Contact information:

Name, address, telephone number, email address:

This template has been adapted from the Template Take Down Notice developed by Jisc, which can be found here: http:/www.jisc.ac.uk/media/documents/themes/content/sca/templatenoticetakedown.pdf