Guidelines on the Disclosure and Barring Service Disclosure Process and Employing Ex-offenders

Contents

Appendices

1. Introduction

The purpose of these guidelines is to provide information on the University's approach to the employment of ex-offenders and the use of Disclosure and Barring Service checks.

Whereas an unspent criminal conviction will not necessarily preclude an individual from employment, managers should always seek advice from the Human Resources Division if they become aware of this. In the event that such a conviction is brought to light or has been declared on the Equal Opportunities form, Section 4 below will apply.

For some posts, it will be appropriate and necessary to undertake a Disclosure and Barring Service check prior to confirmation of appointment.

The Disclosure and Barring Service (DBS) (which merged the Independent Safeguarding Authority (ISA) and the Criminal Records Bureau (CRB)) was established under the Protection of Freedoms Act 2012. It undertakes services to allow authorised users to obtain information about a person's criminal record for approved purposes. Criminal record certificates (known as Disclosures) are issued by the DBS.

Three main types of Disclosure are available in England and Wales:

Standard check - £26
The standard check is available for duties, positions and licences included in the Rehabilitation of Offenders Act (ROA) 1974 (Exceptions) Order 1975, for example, court officers, employment within a prison, and Security Industry Authority (SIA) licences.

A standard level certificate contains details of all spent and unspent convictions, cautions, reprimands and final warnings from the Police National Computer (PNC) which have not been filtered in line with legislation.

Enhanced check - £44
The enhanced check is available for specific duties, positions and licences included in both the Rehabilitation of Offenders Act 1974 (Exceptions Order 1975) and the Police Act 1997 (Criminal Records) regulations, for example, regularly caring for, training, supervising or being solely in charge of children, specified activities with adults in receipt of health care or social care services and applicants for gaming and lottery licences.

An enhanced level certificate contains the same PNC information as the standard level certificate but also includes a check of information held locally by police forces.

Enhanced with a barred list check - £44
The enhanced check with barred list check(s) is only available for those individuals who are carrying out regulated activity and a small number of

positions listed in Police Act 1997 (Criminal Records) regulations, for example, prospective adoptive parents and taxi and Private Hire Vehicle (PHV) licences.

An enhanced level certificate with barred list check(s) contains the same PNC information and check of information held locally by police forces as an enhanced level check but in addition will check against the children's and/or adult's barred lists.

If your application includes a request to check the barred list(s) the DBS has a statutory duty to consider any information that suggests you may pose a risk of harm. We will write to you if you are affected.

Applications for Disclosures may be made only in respect of employment with organisations that have registered with the DBS. Applications must be made by the individual concerned and signed by both the applicant and the registered body.

These notes for guidance set out the procedures to be followed in respect of applications for a Disclosure. UEA as a registered body with the DBS is required to adhere to a strict 'Code of Practice' (available from the Disclosure and Barring Service https://www.gov.uk/government/organisations/disclosure-and-barring-service), which has been designed specifically to ensure that Disclosure information is used fairly, sensibly and confidentially.

2. Employing ex-offenders

The Rehabilitation of Offenders Act 1974 was introduced to ensure that ex-offenders who have not re-offended for a period of time since the date of their conviction are not discriminated against when applying for jobs. It enables ex-offenders to 'wipe the slate clean' of their criminal record in the sense that, unless the post they are applying for is exempted (see below), they are no longer legally required to disclose to organisations convictions that have become 'spent'. Effectively, the Act makes it illegal for an organisation to discriminate against an ex-offender on the grounds of a 'spent' conviction.

The length of time required for an ex-offender to become 'rehabilitated' depends on the sentence received and the age when convicted. Custodial sentences of more than two-and-a-half years can never become 'spent'. Cautions, reprimands and final warnings are not considered to be criminal convictions and so are not covered by the Rehabilitation of Offenders Act.

In order to protect certain vulnerable groups within society there are a large number of posts and professions that are exempted from the Rehabilitation of Offenders Act. These include posts involving access to children, young people, the elderly, disabled people, alcohol or drug misusers and the chronically sick. In such cases, organisations are legally entitled to ask applicants for details of all convictions, irrespective of whether they are 'spent' or 'unspent' under the Rehabilitation of Offenders Act.

The University's policy on the recruitment of ex-offenders is attached at appendix 1.

The following sections set out the procedures for implementing fair, responsible and effective policy and practice for recruiting and retaining people with a criminal record based on a full assessment of the risks involved and are based on good practice recommendations endorsed by the DBS.

3. The recruitment process

At the outset of each recruitment exercise the Human Resources Manager/Senior Adviser/Adviser will consult and advise the recruiting manager whether, given the nature of the job, it is appropriate to ask about criminal records and obtain a Disclosure. Disclosures will be sought only in relation to posts that involve a degree of risk. Disclosure will not be used as a blanket requirement in all circumstances.

Applicants will be asked about criminal records in such a way as to encourage honesty. All applicants are required to complete an Equal Opportunities form which includes the requirement to declare any unspent convictions, providing details in confidence to the Human Resources Manager. Applicants will be informed at the outset if criminal record information will be requested from them. This will provide a basis for the applicant to decide whether or not to apply for the post. Emphasis should be placed on the fact that this information will be used only to assess the applicant's suitability for employment, in so far as it is relevant, and that they will be considered on merit and ability and not discriminated against unfairly.

If an applicant declares an unspent conviction on the Equal Opportunities form, then Section 4, below, will be applied.

When a post has been agreed to require a Disclosure, the following steps are to be followed: -

(a) The job advert must contain a brief statement to make it clear that a Disclosure will be requested in the event of the individual being offered the position, as follows:

This appointment will be subject to a criminal record check from the Disclosure and Barring Service

(b) The University's Statement of Policy on the recruitment of ex-offenders will be included with all job information provided for applicants (Appendix 1).

(c) A brief statement to make it clear that a Disclosure will be requested in the event of the individual being offered the position should be attached to the Application Form, as follows:

Owing to the sensitive nature of this post applicants who are offered employment will be subject to a criminal record check from the Disclosure and Barring Service before the offer of appointment is confirmed. The University of East Anglia aims to promote equality of opportunity for all. Its written policy on the recruitment of ex-offenders is attached for your information. Criminal records will be taken into account for recruitment purposes only when the conviction is relevant. A criminal record will not necessarily bar you from employment. This will depend on the circumstances and background to your offence(s).

(d) The standard application form already requires all applicants to make a statement about criminal convictions. Those who are then invited for interview for a post which has been identified as subject to the Disclosure process will be given the following information and advice in an attachment to the invitation to interview letter:

Owing to the sensitive nature of this post, applicants who are offered employment will be subject to a criminal record check from the Disclosure and Barring Service before the offer of appointment is confirmed. Please note the attached statement of the University's policy on the recruitment of ex-offenders.

The University needs to ensure that the relevance to the role of any information about criminal convictions and associated information about criminal convictions and associated information can be fairly

and confidentially assessed, independently of the normal selection process itself. In order to help ensure this, we encourage applicants to provide details of their criminal record at this stage, separately from the rest of their application.

You should do so by submitting, in a separate envelope marked 'Private & Confidential' and addressed to the Human Resources Manager (DBS), Human Resources Division, University of East Anglia, Norwich, Norfolk, NR4 7TJ, appropriate written details and dates and giving any additional information you wish to draw attention to, which may help to improve our understanding and assist fair decision-making.

The University will expect in such circumstances to discuss, with any candidate being considered for appointment, relevant convictions and associated information. Any such discussion will normally take place in a special interview with one of the University's Human Resources Managers/Senior Advisers.

(e) If the Human Resources Division receives a Private & Confidential communication from an applicant containing such information the relevant Human Resources Manager/Senior Adviser will arrange to discuss it and assess the relevance in a one-to-one interview with the individual concerned <u>after</u> the normal selection interview, if this has led to a recommendation to offer an appointment to the applicant in question. After assessing the relevance of any offence/conviction information to the post applied for, and after appropriate consultation with any third party nominated by the applicant (e.g. a Probation Officer or specialist employment organisation), the Human Resources Manager/Senior Adviser will advise the School or Unit of any relevant issues and review the appointment recommendation in the light of these.

(f) Criminal records information is to be checked and verified using the Disclosure and Barring Service <u>only after</u> the completion of a full assessment of the applicant and at the point of making a job offer. Disclosure checks should not be initiated for all short-listed applicants.

(g) The offer of appointment issued by the Human Resources Division must contain a statement that it is subject to the receipt by the University of a Disclosure from the Disclosure and Barring Service that is satisfactory to the University, and should set out or explain the steps taken in this respect, whether the appointee will be permitted to start work before completion of the process (and any conditions to be attached to this), and the consequence of receipt of a Disclosure which is judged by the University to be unsatisfactory.

The information sent to the appointee must provide a reference to the Guidance Notes for Disclosure Applicants and An Applicant's Guide to Completing the Disclosure, both available on the DBS website:

(**https://www.gov.uk/government/organisations/disclosure-and-barring-service**).

4. Assessing the relevance of criminal records

(a) *In relation to the post*

The suitability for employment of a person with a criminal record will vary, depending on the nature of the job and the details and circumstances of any convictions. Deciding on the relevance of convictions to specific posts is not an exact science. An assessment of an applicant's skills, experience and conviction circumstances should be weighed against the risk assessment criteria for the job. The Human Resources Manager/Senior Adviser and recruiting manager must identify what risks might be involved and what precautions put in place in order to provide satisfactory safeguards, if possible.

To facilitate this process, an applicant's criminal record should be assessed in relation to the tasks he or she will be required to perform and the circumstances in which the work is to be carried out. The following are recommended for consideration (and can be used as a check-list):

- does the post involve one-to-one contact with children or other vulnerable groups as employees, customers and clients?
- what level of supervision will the post holder receive?
- does the post involve any direct responsibility for finance or items of value?
- does the post involve direct contact with the public?
- will the nature of the job present any opportunities for the post holder to re-offend in the place of work?

(b) *In relation to the conviction*

In some cases, the relationship between the offence and the post will be clear enough for the University to decide easily on the suitability of the applicant for the job. It should be remembered that no two offences are exactly alike and whilst it will not be possible to carry out a thorough risk assessment on each individual, it is recommended that the following issues are taken into account as a minimum requirement:

- the seriousness of the offence and its relevance to the safety of other employees, customers, clients and property;
- the length of time since the offence occurred;
- any relevant information offered by the applicant about the circumstances which led to the offence being committed, for example the influence of domestic or financial difficulties whether the offence was a one-off, or part of a history of offending;
- whether the applicant's circumstances have changed since the offence was committed, making re-offending less likely;

- the country in which the offence was committed; some activities are offences in Scotland and not in England and Wales, and vice versa;
- whether the offence has since been de-criminalised by Parliament.

5. Applying for a Disclosure

The Human Resources Division uses an e-bulk system, operated by Atlantic Data Systems, to process DBS applications and Disclosures online. Once an individual has completed the form online the information contained is verified by ADS before being electronically countersigned by an authorised Countersignatory in the Human Resources Division.

The necessary steps in the procedure are set out below and on the Flowchart on the next page.

(a) Following an offer of appointment which specifies that it is subject to a satisfactory Disclosure, the applicant will normally receive an email from the Human Resources Assistant, who will arrange a meeting with the applicant to review proof of identity.

(b) The applicant must attend the Human Resources Division in order for the Human Resources Assistant to review the identity documents and confirm any information relevant for the online application process. The appointee must bring to the meeting the proof of identity as per the DBS list contained within the Gov.uk website; a link to this site is contained within the offer of employment.

Typically this will be a Passport or Driving Licence, plus Birth Certificate, and a recent Utility Bill and Bank Statement.

After the meeting the Human Resources Assistant will enter the details of the identity documents onto the online system and electronically invite the applicant to complete and submit the form online and pay via the UEA Online Store. Once the form has been submitted by the applicant it will undergo a verification check by ADS. Once the verification stage has been completed and payment made the form will be countersigned and sent to the DBS electronically.

(c) The DBS will send the Disclosure document to the applicant, and UEA will be able to review online whether the Disclosure contains any information. If it does not contain any information then the offer will be confirmed accordingly. If it does contain any information then the applicant will be asked to bring the original Disclosure into the Human Resources Division within two weeks.

APPLYING FOR A DISCLOSURE - FLOWCHART

Disclosure required

↓

Refer to Policy Statement on the Recruitment of Ex-Offenders

↓

Human Resources Assistant will contact the applicant to arrange a meeting for the applicant to bring in their identity documents

↓

Applicant will attend meeting with Human Resources Assistant who will check proof of identity documents and initiate the online application process

↔ Proof of **Identity**, typically:

- Passport, **or**
- Driving licence **and**
- Birth Certificate

↔ Proof of **Address**, typically:

- Bank statement **and**
- Utility bill

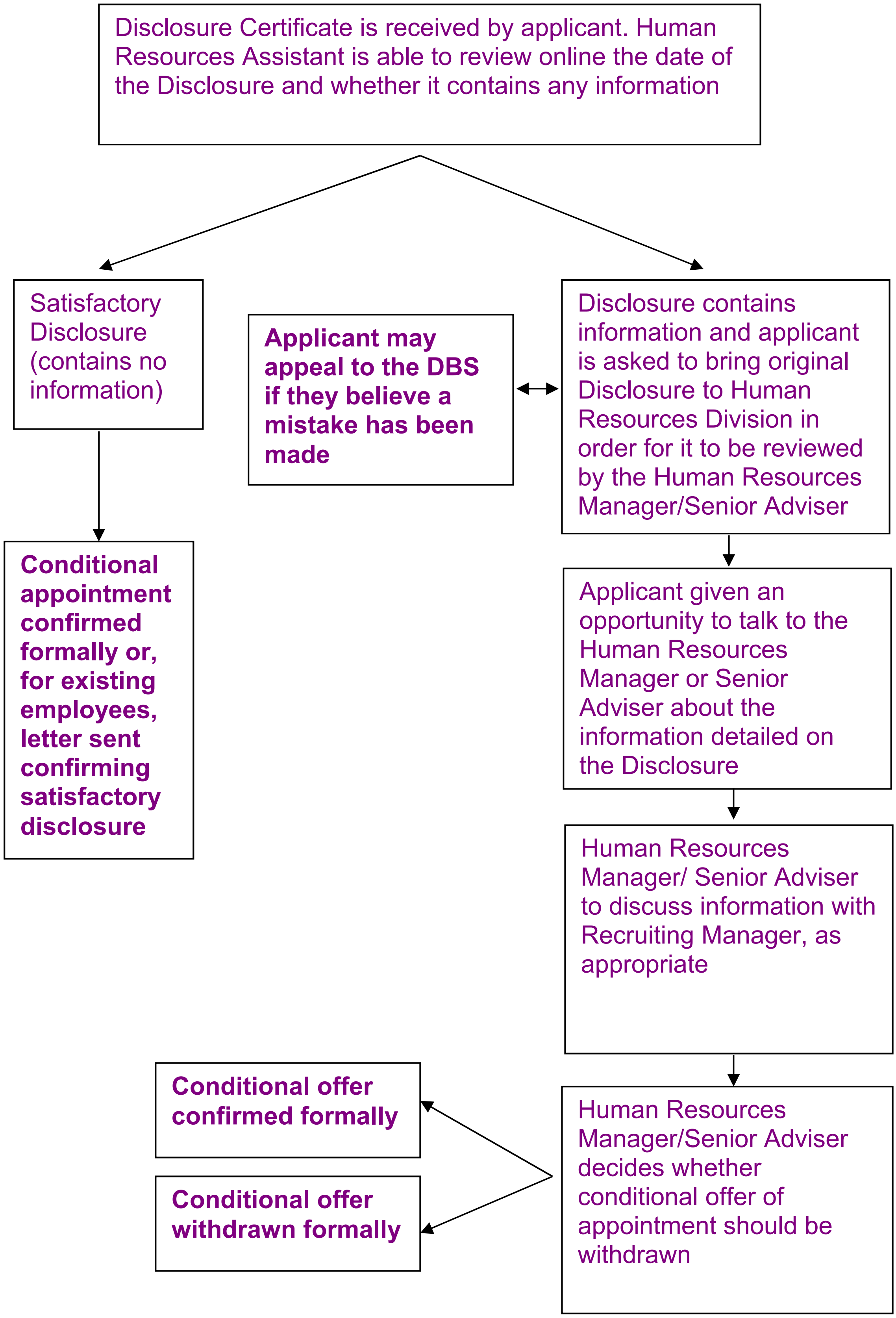
↓

Applicant completes the application online, makes payment using the online payment facility and submits electronically, the form is then verified by ADS

↓

Completed form is electronically countersigned and sent to the DBS electronically

RETURN OF DISCLOSURE - FLOWCHART



6. Alternative methods of obtaining a Disclosure

a) The applicant may be able to present a recently issued DBS Disclosure Certificate for assessment. This is acceptable, provided it is in good condition and was issued no more than three months prior to the date on which it is presented to the Human Resources Division.

b) The DBS offers an update service which allows applicants to keep their DBS certificates up to date and take their certificate from one job to the next. The service allows employers to check a DBS certificate online free-of-charge. Applicants need to register in order to use this service and pay £13 per year to maintain their subscription. Applicants registered to use this service should alert Human Resources on receipt of their offer letter and give their permission for a Countersignatory to perform a status check. In addition, the applicant will need to confirm their Disclosure Certificate number, the surname used on the certificate and their date of birth.

7. Assessing Disclosures

If the Disclosure contains information about a criminal record and/or if it contains information which is consistent with that provided by the applicant during the selection process the Human Resources Manager/Senior Adviser concerned will decide whether the job offer is to be confirmed in the light of the Disclosure or whether a further discussion with the applicant must take place (which may lead to the withdrawal of the original offer of appointment). This may involve consulting the relevant recruiting manager.

It may be that the Disclosure contains information the applicant was not asked about during the interview, or the applicant was unaware they had a criminal record. It may be they have been given inaccurate information and are under the impression their convictions have become spent under the terms of the Rehabilitation of Offenders Act. (Sentences of the court can be extremely complex and it is frequently the case that offenders do not understand the nature of the sentence(s) they have received.) It may be they hid their convictions in order to increase their chances of employment.

Alternatively, it may be that the information contained in the Disclosure is inaccurate, or relates to someone else with the same name. (Applicants are entitled to appeal to the DBS if they think a mistake has been made. Guidance on the Appeals process can be on the DBS web site or alternatively from the DBS Help line). In any event, applicants should be given the opportunity to explain the situation wherever possible in a face to face discussion with the Human Resources Manager/Senior Adviser before a final decision is made.

In making a decision, the Human Resources Manager/Senior Adviser will have regard to the particular circumstances and to the general issues set out in the earlier section on assessing the relevance of criminal records.

8. Guidelines on complying with storage, handling and confidentiality requirements

The University has adopted a formal policy on the Secure Storage, Handling, Use, Retention & Disposal of Disclosures & Disclosure Information Including Use of the e-Bulk Service, which is set out in Appendix 2.

All those members of the University who are involved in the DBS process must be made aware of the policy and understand that it is a criminal offence to pass Disclosure information to anyone who is not authorised to receive it.

A copy of the Policy Statement must be made available to any applicants or others who wish to see it.

Appendix 1

Statement of Policy on the Recruitment and Employment of Ex-Offenders

1. For posts subject to a DBS Disclosure

As an organisation using the Disclosure and Barring Service (DBS) to assess applicants' suitability for positions of trust, the University of East Anglia complies fully with the DBS Code of Practice and undertakes to treat all applicants for positions fairly. It undertakes not to discriminate unfairly against any subject of a Disclosure on the basis of conviction or other information revealed. This statement of the policy on the recruitment of ex-offenders will be made available to all Disclosure applicants at the outset of the recruitment process.

- We actively promote equality of opportunity for all with the right mix of talent, skills, and potential and welcome applications from a wide range of candidates, including those with criminal records. We select all candidates for interview based on their skills, qualifications, and experience.
- A Disclosure is only requested after a thorough risk assessment has indicated that one is both proportionate and relevant to the position concerned. For those positions where a Disclosure is required, all application forms, job adverts and recruitment briefs will contain a statement that a Disclosure will be requested in the event of the individual being offered the position.
- Where a Disclosure is to form part of the recruitment process, we encourage all applicants called for interview to provide details of their criminal record at an early stage in the application process. We request that this information is sent under separate, confidential, cover to a designated person within UEA and we guarantee that this information is only be seen by those who need to see it as part of the recruitment process.
- Unless the nature of the position allows the University of East Anglia to ask about your entire criminal record we only ask about "unspent" convictions as defined in the Rehabilitation of Offenders Act 1974.
- We ensure that all those in The University of East Anglia who are involved in the recruitment process receive suitable training and guidance to identify and assess the relevance and circumstances of offences. We also ensure that they have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, e.g. the Rehabilitation of Offenders Act 1974.
- At interview, or in a separate discussion, we ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. Failure to reveal information

that is directly relevant to the position sought could lead to withdrawal of an offer of employment.

- We make every subject of a DBS Disclosure aware of the existence of the DBS Code of Practice and make a copy available on request.

- We undertake to discuss any matter revealed in a Disclosure with the person seeking the position before withdrawing a conditional offer of employment.

- Having a criminal record will not necessarily bar you from working with the University of East Anglia. This will depend on the nature of the position and the circumstances and background of your offences.

2. All posts, including those not subject to a DBS Disclosure

The University of East Anglia is committed to being an Equal Opportunity employer and this policy aims to ensure that ex-offenders receive fair treatment throughout their experience of recruitment and employment with the University.

In addition to the process outlined within section 4 of these Guidelines when an applicant for a post declares an unspent conviction, sometimes circumstances affecting an individual’s criminal record status change during the course of employment. Therefore, once in employment, staff must inform their line managers and/or Human Resources of such a change in confidence in order that the impact upon their suitability to undertake their role may be reviewed. Line managers must bring any such circumstances to the attention of the Human Resources Manager/Senior Adviser/Adviser in order that an assessment of the relevance of any conviction can be undertaken.

Appendix 2

Statement of Policy on the Secure Storage, Handling, Use, Retention & Disposal of Disclosures & Disclosure Information Including Use of the e-Bulk Service

This policy for the secure storage, handling, use, retention and disposal of Disclosures and Disclosure information including use of the e-Bulk service is provided in order to comply with current regulations.

General Principles

As an organisation using the Disclosure and Barring Service (DBS), the University of East Anglia complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. We also comply fully with its obligations under the Data Protection Act (DPA) and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure information.

Handling

In accordance with Section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and we recognise that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Storage and access

1. *Paper-based Disclosures*

   A paper-based Disclosure Certificate is never kept on an applicant's personal file and is always stored securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. Disclosure Certificates are only requested if they contain information and are retained temporarily whilst the applicant's criminal record is assessed. Once the assessment is complete, the Certificate is safely returned to the applicant.

2. *E-Bulk (electronic) Disclosures*

   Electronic disclosure information is held on a secure password-protected system accessible only to those authorised to view it in the course of their duties. Data contained within the system is not saved into any format outside of the online system and is not stored separately, scanned, emailed or distributed.

3. *Risk assessments*

Risk assessments are undertaken when a Disclosure is received that contains information. The documents are stored electronically and access is restricted to Countersignatories, with secure password controls in place.

4. *ID documents*

Identify documents are seen and verified, by those who are authorised to do so in the course of their duties, for the purpose of obtaining a Disclosure. Copies of these documents are not retained.

Usage

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Lost criminal records checks

If a Disclosure, or related information, is lost, the University will inform the DBS immediately.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, The University will give full consideration to DBS guidance, the Data Protection Act and Human Rights Act before doing so. Throughout this period the conditions regarding appropriate, safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, the University will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Disclosure certificates received electronically through the e-bulk system are automatically deleted from the system after 180 days. Risk assessments stored electronically are manually deleted from the electronic filestore after 180 days.

If online applications are not completed in full, they are removed from the system in compliance with the Data Protection Act. A 20 day reminder message and 30 day prompt to cancel an application is provided to the University by ADS and after 345 days automatic system removal and data purge occurs.

Appendix 2

Statement of Policy on the Secure Storage, Handling, Use, Retention & Disposal of Disclosures & Disclosure Information

This Policy explains [University of East Anglia's] position on the secure storage, handling, use, retention & disposal of disclosure information.

[University of East Anglia] ("we", "us" and "our") refers to the Registered Body who is responsible for the applications processed through this website, whose registered office is [University of East Anglia, Norwich Research Park, Norwich, NR4 7TJ].

We reserve the right to revise this policy or any part of them from time to time, so you should review these terms periodically for changes.

General Principles: As an organisation using the services of the Disclosure and Barring Service, Disclosure Scotland and Access NI we agree to comply fully with their respective Codes of Practice, in particular with regard to the correct handling, use, storage, retention and disposal of disclosures and disclosure information.

We also comply fully with our obligations under data protection legislation, including the Data Protection Act, the General Data Protection Regulation and all other relevant legislation relating to the safe handling, use, storage, retention and disposal of disclosure information.

Handling: In accordance with section 124 of the Police Act 1997, disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom disclosures or disclosure information has been revealed and we recognise that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Access: System access is only granted to authorised personnel, which ensures that access to disclosure information is only available to individuals who are involved in the employment decision. Access is only available with username and password protection to prevent unauthorised access or modification.

Scanning/copying of DBS information: Where an applicant presents a previously completed disclosure certificate and supporting details, for example to access the DBS Update Service, we shall only scan/copy a disclosure certificate with the permission of the applicant. To scan/copy a disclosure certificate that contains information that we are not entitled to see - either children's barring information or adult barring information - is not permitted and could constitute a breach of the applicant's rights under data protection legislation.

Printing of disclosure information: Communication of disclosure result information (verbal, written, or by email etc.) must only be between individuals who are involved in the employment decision or are entitled to access disclosure information as a part of their ordinary duties.

DBS result information must be printed no more than once and is only available with username and password protection to prevent unauthorised access or modification.

Readable copies may be printed for the purpose of presenting them to relevant industry regulatory inspectors at the time of an inspection. Where applicable this may include, for example, auditors/inspectors from the Department for Education (DfE), Ofsted, Care Quality Commission (CQC), Care Inspectorate Wales (CIW), Financial Standards Authority (FSA)/Financial Conduct Authority (FCA), Law Society, Solicitors Regulation Authority.

Forwarding of electronic disclosure information: Forwarding of disclosure result information is not permitted on the system. Documents may not be saved into any format outside of the online system and cannot be stored separately electronically, emailed or distributed.

Usage: Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Loss of Documents: If disclosure information is lost, such loss must be reported to Atlantic Data Ltd or the registered body countersigning the application, stating what has been lost, how, in what format and by whom.

Failure to comply with this policy could result in:

- a non-compliance notice being issued and a requirement to remedy and provide evidence of the remedial action within 14 days
- suspension of the user(s) from the account
- suspension or termination of the online account.

Storage: Disclosure result information, whether a disclosure certificate, electronic result information, printed result information or scanned/copied result information must be handled in accordance of the relevant Codes of Practice. We ensure that every user is provided with this policy statement on the secure storage, handling, use, retention and disposal of disclosure information, as well as full access to the DBS Code of Practice.

5. Paper-based Disclosures

A paper-based Disclosure Certificate is never kept on an applicant's personal file and is always stored securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. Disclosure Certificates are only requested if they contain information and are retained temporarily whilst the applicant's criminal record is assessed. Once the assessment is complete, the Certificate is safely returned to the applicant.

6. E-Bulk (electronic) Disclosures

Electronic disclosure information is held on a secure password-protected system accessible only to those authorised to view it in the course of their duties. Data contained within the system is not saved into any format outside of the online system and is not stored separately, scanned, emailed or distributed.

7. *Risk assessments*

Risk assessments are undertaken when a Disclosure is received that contains information. The documents are stored electronically and access is restricted to Countersignatories, with secure password controls in place.

8. *ID documents*

Identify documents are seen and verified, by those who are authorised to do so in the course of their duties, for the purpose of obtaining a Disclosure. Copies of these documents are not retained.

Retention: We do not keep disclosure information for any longer than is necessary. Original and scanned/copied disclosure certificates will be kept for a maximum of 6 months to allow for the employment decision to take place and for the consideration and resolution of any disputes or complaints.

If circumstances dictate that is necessary to keep disclosure information for longer than 6 months, this will be for a period of no longer than 12 months. This must also be with the prior agreement of the applicant. We will also consult the DBS and will give full consideration to the data protection and human rights of the individual before doing so.

Original certificates or printed disclosure result information may be retained in exception to the 6 month retention period in circumstances where an industry regulator has a statutory or legal right to audit disclosure result of relevant personnel. Such examples include:

- Adult care home or domiciliary care services regulated by the CQC
- Schools or nurseries regulated by DfE and/or Ofsted
- An organisation working with or within an NHS Trust or Hospital in compliance with the NHS employer check standards.

DBS application information within the e-bulk system: The data processor (Atlantic Data Ltd.) does not keep applicant data for any longer than is necessary. The personal data forming a basic record of an application will be retained as a record of the application for up to 7 years. This includes the applicant’s name, address, date of birth, and contact details. Supporting information provided as part of the disclosure application, such as identity documents, previous names and addresses will be purged from the system after 1 year. The University of East Anglia may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the employment decision taken. This information will be retained on the applicant’s personal file and will be destroyed in accordance with the departmental retention schedule, should the applicant leave their employment/course of studies with the University of East Anglia.

Disposal:
Manual Disposal Methods - once the retention period has elapsed, we will ensure that any disclosure information is destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

Shredding is conducted at a ‘Level 4 (DIN 4)’ standard.

We will not keep any photocopy or other image of the disclosure or any copy or representation of the contents of a disclosure. No electronic copies of disclosure certificates will be retained in any electronic format.

Electronic Disposal Methods - a secure erase method is used using utilities such as "shred" and "delete". The shred command is executed in Linux based systems to securely delete files by overwriting the contents of the file with junk data. Shred will securely delete the given file by overwriting it first with random data 30 times and then with (zeros), afterwards it will remove the file. Shred can also erase the whole partition using 7 iterations with random numbers. Also, it writes zeros to hide the shredding process at the end.

Disk sanitisation – at data base level - Disk sanitisation involves securely erasing all the data from a disk so that the disk is, except for the previous wear, “new” and empty of any previous data.

Disk Erase – at hard drive level – the operating system is installed only on encrypted drives, using dm-crypt and LUKS. We use a tool that can erase disks called "Darik's Boot & Nuke", this allows to sanitize installed operating system as well as other attached disks.

The other procedure to securely remove confidential data from disks is to destroy the disk. This destruction may be either magnetic or physical. Magnetic destruction involves applying a strong magnetic field to the disk that erases all data. This process often destroys disk read/write heads so the disk cannot be used again. Physical destruction involves either taking apart the disk and cutting the platters into small pieces or otherwise destroying the disk (e.g., high temperature or crushing).

Acting as an umbrella body: Before acting as an umbrella body (an umbrella body being a registered body which countersigns applications and receives disclosure result information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that our clients will store, handle, use, retain and dispose of disclosure information in full compliance with the relevant Codes of Practice and in full accordance with this Policy.

We will also ensure that any organisation or individual, at whose request applications for disclosures certificates are countersigned, has such a written policy and, if necessary, will provide a sample policy for that body or individual to use or adapt for this purpose.