



Policy name: Access to Digital Evidence (A2DE) Policy Framework

Reference: N/A

Re-Issue Date: 13 February 2025

Implementation Date: 21 December 2018

Introduces amendments to the following documents (e.g., PSIs, PSOs, Custodial Service Specs): None

Action required by:

<input type="checkbox"/>	HMPPS HQ	<input checked="" type="checkbox"/>	Governors / Directors
<input checked="" type="checkbox"/>	Public Sector Prisons	<input type="checkbox"/>	Heads of Group
<input checked="" type="checkbox"/>	Contracted Prisons	<input type="checkbox"/>	Contract Managers in Probation Trusts
<input type="checkbox"/>	National Probation Service	<input type="checkbox"/>	HMPPS-run Immigration Removal Centres (IRCs)
<input type="checkbox"/>	HMPPS Rehabilitation Contract Services Team	<input type="checkbox"/>	Other providers of Probation and Community Services

Mandatory Actions: All groups referenced above are required to adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information: Governors / Directors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public Sector Equality Duty (Equality Act, 2010).

Audit/monitoring: This Policy Framework will be reviewed at yearly intervals. Please send feedback to the HMPPS Security Procedures functional mailbox.

Resource Impact: Highly limited as this is process which is currently being carried out under guidance notes. Prison Governors will appoint a designated Single Point of Contact (SPOC) from the Senior Leadership Team (SLT) whose responsibility will be to ensure appropriate staff are in place to manage A2DE in the establishment.

Contact: Access to Digital Evidence Team: A2DENational.Belmarsh@Justice.gov.uk
HMPPS Security Procedures Team: security.procedures@justice.gov.uk

Deputy/Group Director sign-off: Andy Rogers, Deputy Director of Security, August 2023

Approved by OPS for publication: Phil Cople, Joint Chair, OPS, December 2018

Revisions

Date	Update
October 2023	More defined terms of who is eligible and why and under what conditions, and including the introduction of a dedicated A2DE HMP Belmarsh mailbox.
13 February 2025	Paragraph 19.8 updated.

CONTENTS

Section	Title	Page
1	Purpose	3
2	Outcomes	3
3	Article 6, Human Rights Act 1998	3 - 4
4	Requirements (Determining Approval)	4 - 6
5	Requirements (After Approval)	6 – 7
6	Constraints	7
7	Guidance	8
8	Appeals against Sentences and Convictions	8
9	Inappropriate Material	8 - 9
10	Risk Factors	9
11	Summary of Legal Disclosure & Rule 39 Mail	10
12	Searching of A2DE Equipment	11
13	Procedure after A2DE equipment is removed	11
14	Legal Teams handing in Electronic Documents via Court	12
15	IT Evidence received via the post	12
16	Secure viewing of all TACT cases	12 - 13
17	Secure viewing of all non-TACT cases	13
18	A2DE provided to Another Government Agency	14
19	Auditable Recording of all A2DE Equipment	14 - 15
20	Records Management for A2DE	15
Annex A	Application Form	
Annex B (1)	Response to Prisoner (In Possession)	
Annex B (2)	Response to Prisoner (Secure)	
Annex C	Inappropriate Material	
Annex D (1)	Compact for the use of A2DE equipment (In Possession)	
Annex D (2)	Compact for the use of A2DE equipment (Secure)	
Annex E	Security Checks	
Annex F	Compact for the use of A2DE equipment monthly reviews	
Annex G	Refusal of Equipment	
Annex H	Removal of Equipment	
Annex I	Risk Assessment for Secure Viewing	
Annex J	The Role of the A2DE Coordinator	
Annex K	A2DE Process Flow Chart – HMP Belmarsh	
Annex L	A2DE Process Flow Chart – Other Prisons, STC's & STH's	

1. Purpose

- 1.1 This Policy Framework sets out the process for Governors / Directors in providing prisoners with A2DE equipment (Information Technology equipment), where that equipment is required for prisoners to view electronic disclosure by the Crown of evidence for the prosecution in any criminal case. Equipment provided for these purposes is termed Access to Digital Evidence (A2DE) Equipment.
- 1.2 Electronic disclosure is defined as electronic information disclosed by the Crown as evidence for the prosecution in a criminal case against a prisoner.
- 1.3 This policy is intended to give clarity to Governors / Directors regarding the requirements that they must comply with surrounding prisoners' A2DE in both public and private sector prisons and to make clear the expectations of HMPPS surrounding prisoners' A2DE in the light of obligations under Article 6 of the European Convention on Human Rights (right to a fair and public hearing).
- 1.4 If prisoners do not receive access to evidence to allow them to prepare for a criminal trial, as they are entitled to, then there is a risk that trials will collapse.
- 1.5 To allow prisoners access to A2DE equipment introduces a potential threat to security that requires a considerable resource to manage and if a prisoner's legal work can be adequately conducted without it (i.e., using paper and pen) then that is the safest (and preferred) option.
- 1.6 Collapsed trials due to defendants' inability to prepare adequately for a trial may harm the public interest. However, the potential misuse of A2DE equipment and risks attached to this mean that the benefits of A2DE access should be carefully balanced against costs and risks.
- 1.7 The purpose of providing the equipment is not to simply facilitate swifter communications or to make correspondence and/or submissions more presentable. Nor is it solely to make the manipulation of digital material easier. Rather, it is to prevent the impediment of access to material that might result if the equipment was not made available.
- 1.8 It is mandatory that Governors/ Directors follow this Policy Framework.

2 Outcomes

- 2.1 Prisoners receive A2DE assistance which they are entitled to, in line with this Policy Framework.
- 2.2 Governors and Directors, through appropriate trained staff, are able to appropriately handle requests from prisoners requesting A2DE equipment.
- 2.3 Prison Governors and Directors will appoint a designated Single Point of Contact (SPOC) from the Senior Leadership Team (SLT), whose responsibility will be to ensure appropriate staff are in place to manage A2DE in the establishment. **Annex J** provides further information regarding the A2DE role.

3 Article 6, Human Rights Act (HRA) 1998 and Article 6, European Convention on Human Rights (ECHR)

- 3.1 Article 6 of the HRA 1988 reflects Article 6 of the ECHR and provides all individuals the right to a fair and public hearing.

- In the determination of their civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order, or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
- Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
- Everyone charged with a criminal offence has the following minimum rights:
 - a) to be informed promptly, in a language which they understand and in detail, of the nature and cause of the accusation against them.
 - b) to have adequate time and facilities for the preparation of their defence.
 - c) to defend himself in person or through legal assistance of their own choosing or, if they have not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require.
 - d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on their behalf under the same conditions as witnesses against them.
 - e) to have the free assistance of an interpreter if they cannot understand or speak the language used in court.

3.2 Whilst this Policy Framework is directed at criminal matters that attract the protections of Article 6 of the ECHR and Article 6 of the Human Rights Act 1998, we recognise that there may be exceptional circumstances outside of the Policy Framework where a civil matter may also attract Article 6 rights. Any application on these matters will need to be considered on a case-by-case basis, against the criteria assigned in this Policy Framework for criminal matters such as the nature of the material to be viewed and the volume of documents. Applications will need to be sent to the National A2DE Team at HMP Belmarsh who will then seek further advice from procedures and legal, as necessary. Where possible, prisons should first consider alternative methods for viewing civil case material.

4 Requirements (Determining whether to allow A2DE)

- 4.1 Governors and Directors are required to ensure that systems are in place to alert prisoners to this Policy Framework on Access to Digital Evidence (A2DE) equipment.
- 4.2 Governors and Directors are required to ensure that all prisoners allocated A2DE equipment are managed in accordance with this Policy Framework.
- 4.3 Any A2DE must not contravene the Prison Service's duty to protect the public, the victims of crime, other prisoners and prison service staff as detailed in the Public Protection Manual.
- 4.4 When handling a request for A2DE equipment, the National A2DE Team at HMP Belmarsh is required to consider whether a prisoner will genuinely be disadvantaged without access to the appropriate equipment.
- 4.5 If prisoners are defending themselves, it does not necessarily follow that A2DE equipment must be provided for the duration of the case (if at all) – for example, it might only be needed to view one piece of evidence and so should be withdrawn as soon as possible afterwards.
- 4.6 The Governor / Director is required to ensure that an establishment risk assessment is carried out and is in place to mitigate any risks involved in the use of A2DE equipment.

- 4.7 A prisoner's request for A2DE equipment facilities may be approved if:
- 4.7.1 It is in order to view evidence only available digitally and fits the A2DE criteria to prepare their defence in a criminal prosecution.
- 4.7.2 All A2DE criteria must be approved in accordance with **Section 5**.
- 4.8 An application **will not** be approved if:
- a) The prisoner wishes to type letters to their legal team rather than write them by hand for their trial or personal defence.
 - b) The prisoner wants the equipment purely to view video or listen to audio evidence on that does not fit the A2DE criteria. This can be accessed during a legal visit with their solicitor.
It is prohibited for prisoners to have evidential discs/ USBs/ hard drives in possession to listen to or view.
 - c) The prisoner would not be competent or able to use the equipment provided. This will be determined by the prisoner or legal team informing us if the applicant is not computer literate.
 - d) The appellant is appealing against sentence.
 - e) The prisoner is preparing an application to appeal against conviction, but no live appeal is current, and the prisoner has not been given a live appellant number.
 - f) The prisoner claims their disability does not allow them to write and would need a typing aid. In this case the preferred option is for the prisoner to purchase their own electronic typewriter.
 - g) The evidence can be viewed in a non-digital or paper format, then the normal procedures for handling correspondence will apply, including Rule 39/ Confidential Access procedures depending on the identity of the sender. (See **Authorised Communications Controls and Interception Policy Framework & Prisoner Communication Services PSI 49/2011**)
- 4.9 Once approved, the prisoner will be granted access to the A2DE equipment for the period specified. Whether such access has to be in-possession or secure viewing will depend on the outcome of the risk assessment – see **Annex K**.
- 4.10 Governors and Directors are required to ensure that an appropriate named SPOC is identified for the establishment, that staff are afforded the required time to complete this task, and that they will be provided appropriate time to attend the A2DE training provided by the National A2DE Team at HMP Belmarsh.
- 4.11 Governors and Directors are required to ensure that prisoners do not have in-possession any inappropriate material as part of the disclosed evidence (**See Section 10 - Inappropriate Material & Annex C**) and which therefore could be shared with other prisoners.
- 4.12 Where it is decided that a prisoner is eligible for A2DE equipment, this will only be in "read only" access - i.e. A2DE equipment that has been configured to HMPPS standard to allow a prisoner to read material but has had all other functions and applications disabled (including "write" access). (See **Section 11 - A2DE Risk Factors**).
- 4.13 Where the prisoner has voluminous amounts of electronic data, it may make it difficult for the prisoner to participate in the proceedings without the use of A2DE equipment. The equipment will be read only, and all annotations are to be in paper format.
- 4.14 A2DE will be considered, and a decision will be made on a case-by-case basis by the National A2DE Team at HMP Belmarsh which comprises complexity and volume of the material served by the Crown. This should be a **minimum of 3500 pages** of evidence, excluding CCTV & audio evidence. Timescales for the sifting of submitted data will be dependent on the volume,

complexity and format of the material provided. We will work to a period of a minimum of 10 working days to complete the sift but this may be extended when required.

4.15 Evidence **may** be considered only if:

- a) The evidence in the criminal case has been submitted by the Crown in electronic format and is too voluminous to be viewed in paper format or during a legal visit.
- b) To have the amount of relevant disclosure in possession would breach the establishments' volumetric controls, unless under 3,500 pages. Please note not all disclosure is relevant and most can be viewed with a legal representative during a legal visit.
- c) The defence is complex or requires the investigation of data that could not easily be carried out without the use of the equipment provided.
- d) The prisoner has a particular disability which would inhibit them from viewing the evidence in paper format.
- e) The information is sensitive and in a format that could only be viewed by using A2DE equipment. For example, a secure video that contains inappropriate material listed in **Annex C** of the Policy Framework.
- f) The prisoner has a live appeal with a valid appeals court number and is appealing against conviction. Where new additional disclosure is available, which could cast doubt on the conviction, the material must still meet the A2DE criteria.

4.16 Any requests for consideration outside of this policy, such as a prisoner with a specific disability, should be made in writing to the A2DE mailbox: **A2DENational.Belmarsh@Justice.gov.uk**, who will consult with the policy lead: **security.procedures@justice.gov.uk**

5 Requirements – after approval

Once the decision has been taken to provide A2DE equipment, the following requirements must be observed.

- 5.1 All A2DE equipment must be to the approved HMPPS specification. The approved specification equipment can be only obtained through the National A2DE Team at HMP Belmarsh.
- 5.2 A2DE equipment must only contain prosecution materials issued by the Crown Prosecution Service (CPS), Police or legal teams. This must be sifted before being loaded onto the prisoners' equipment for any inappropriate material. Disclosure DVD / CD disks must not be allowed in the prisoner's possession at any point. No Rule 39 material will be loaded onto the A2DE laptop.
- 5.3 Any member of staff responsible for this area of work are required to have the appropriate level of training and knowledge, requiring attendance at HMP Belmarsh for training. (See **Annex J - The Role of the A2DE Co-ordinator**).
- 5.4 All A2DE applications (both accepted and refused) are required to have an auditable paper trail.
- 5.5 All A2DE paperwork is required to be managed in accordance with the HMPPS Records Retention & Management; PSI 04/2018. (See **Section 21 - Records Management for A2DE**).

- 5.6 Searching procedures for A2DE Equipment is required to be in accordance with A2DE searching protocols. (See **Section 13 - Searching of A2DE Equipment**).
- 5.7 In the event that legal teams hand in further material for disclosure, the protocol for receiving of media (CD/DVDs') from legal representatives is required to be followed. (See **Section 15 - IT Evidence** received via the post).
- 5.8 If a prisoner refuses to accept the A2DE equipment offered to them, possibly because the prisoner wants fully open equipment with USB facilities and full write access, then **Annex G, Refusal of Equipment** is required to be completed.
- 5.9 If a prisoner decides before their sentencing that they no longer want the A2DE equipment as they have been found or pleaded guilty, then **Annex H (Removal of Equipment)** must be completed. See **Annex E (Security Checks)** for purging procedure after removal. This will fully close the A2DE application and any further submissions of material in their case will need to be viewed with their legal representatives.
- 5.10 All stages of the process from application to removal of equipment (end to end) are required to be documented and retained (in the core record) in case of legal challenge or in cases where the court, defence or prosecution query the procedures followed.
- 5.11 Governors and Directors are required to ensure that all inappropriate material (**Annex C - Inappropriate Material**), and legal undertakings are viewed only under secure viewing conditions and never allowed in possession.

6 Constraints

- 6.1 All A2DE systems are required to meet the HMPPS Specification of A2DE equipment. The approved specification equipment can be only obtained through the National A2DE Team at HMP Belmarsh.
- 6.2 The equipment provided by the National A2DE Team at HMP Belmarsh does not allow write access on the systems for prisoners. If write access were to be allowed and annotations made upon the A2DE equipment, the entire system would be covered by Prison Rule 39. This would nullify the ability to carry out the necessary interrogation of our systems and networks including security checks and would therefore exist outside of this Policy Framework.
- 6.3 The equipment provided by the National A2DE Team at HMP Belmarsh will ensure that Wi-Fi and USB ports are totally disabled for security purposes. (See **Section 11 - for Risk Factors**).
- 6.4 A2DE equipment is not for the provision of any Rule 39 correspondence. A2DE equipment must not contain any documentation that may be deemed as Prison Rule 39. For example, legal letters from a solicitor to their client or from a defendant to their legal team. (See **Section 11 - Summary of Legal Disclosure & Rule 39 Mail**).
- 6.5 Electronic disclosure viewed on A2DE equipment is read only. The equipment does not facilitate write access. A2DE is only suitable for the provision of electronic information that has been disclosed in open court, so it is not covered by Rule 39 Legal Privilege and may be viewed by staff.
- 6.6 Applications for an A2DE equipment will not be considered or processed if the trial is a criminal case and has already commenced. The material should already have been provided to the prisoner, from their legal team prior to the start of their case. A2DE is set up to allow preparation for the trial and if an application is received when the trial has started it cannot be considered preparation. Additionally, the application process can take around 6 weeks to

complete and therefore would not provide the required assistance for the trial in a timely manner.

- 6.7 Once the prisoner has been sentenced in the criminal court, they may wish to use A2DE equipment in the context of a confiscation order (POCA) issued by that court or any other separate criminal proceedings. In all cases the POCA will be treated as a new legal matter that concerns the original case that may therefore require some or all of the original materials, and a new application will be required. If it is confirmed that the POCA hearing is scheduled within a three-month period following sentence, the A2DE equipment will continue to be loaned under the same conditions as in the existing Compact **Annex D1 /D2**, and the new application must include a copy of the court communications confirming the date of POCA scheduling.
- 6.8 If it is confirmed that the POCA/ confiscation order hearing is scheduled outside of a three-month period from the date of sentencing, or where a POCA hearing date is unknown the machine will be removed and returned to the A2DE team with the drive being purged. A new application will then be required when the date is fixed, with the application only being approved three months prior to the POCA hearing date, having provided evidence of the court scheduling date.

7 Guidance

- 7.1 Prisoners' A2DE needs are to be balanced against security and safety considerations. A2DE access may be restricted where it is necessary for safety reasons to secure good order and discipline, prevent crime or protect victims.
- 7.2 Staff will also need to be aware that the preparation for trial may sometimes cause distress. This may be because in the receiving and reviewing of the link with past trauma or reaffirm previous actions such as those of a violent or sexual nature. Staff need be aware of these potential risks and triggers ensure relevant support is offered accordingly.
- 7.3 HMPPS is **not** obliged to provide A2DE or allow A2DE to be provided (see Article 6, Section 3) unless the prisoner or legal representative requesting it on behalf of the prisoner satisfactorily demonstrates that refusing the request would raise a real risk of prejudicing the specific criminal legal proceedings.
- 7.4 Electronic disclosure is defined as electronic information disclosed by the Crown submitted by the Crown as evidence for the prosecution, and which formulates the basis of any criminal case.

8 Appeals against sentences and convictions

- 8.1 Neither of the following two processes would require the use of A2DE equipment:
- The Crown Court has the power to alter a sentence or other order made by the Crown Court within 56 days of the date on which it was made, (Section 155 Powers of Criminal Courts (Sentencing) Act 2000, as amended by section 47 and schedule 8 paragraph 28 Criminal Justice and Immigration Act 2008). This allows time for the correction of errors that would otherwise require an appeal to the Court of Appeal.
 - Before any appeal can commence an appellant is required to serve an appeal notice (Form NG Notice and Grounds of appeal) on the Crown Court office not more than 28 days after the conviction, sentence, or order in accordance with Criminal Procedure Rules 68.2. There is no requirement for the appellant or their solicitor to serve notice on the respondent of an intention to appeal. Neither process would require the use of A2DE equipment.

- 8.2 However, as soon as an appellant has been granted leave to appeal against conviction the Criminal Appeal Office (CAO) will forward to the CPS of the relevant area written notification of the granting of the leave to appeal. This will be accompanied by a copy of the appeal papers, for immediate onward transmission to the CPS office dealing with the case. From this point onwards, the appellant may make an application for A2DE equipment which should be assessed in the same manner as any new A2DE application. Please note that we will not allow the appellant to type on this system. In the rare event that typing is necessary then a typewriter may be considered.
- 8.3 An A2DE application for an appeal against conviction should only be considered 'live' if leave to appeal against conviction is granted and a valid appellant number is provided.

9 Inappropriate material

- 9.1 No material listed below will be allowed in possession and secure viewing protocols should be used to view such material: *
- a) Video, audio, or picture files, containing or depicting any violent act that appears to glorify acts of terrorism. For example, suicide bombings or executions, audio by any radical preacher, cleric, or any radical audio from any religious denomination.
 - b) Video, audio, or picture files containing or depicting any violent act that appears to glorify acts of extreme violence, this could include gang culture video's (known as drill videos).
 - c) Video, audio, or picture files of a graphic nature. Graphic material is defined as any material that may cause alarm, distress or harm to any individual that is exposed to the content.
 - d) Any material subject to a signed legal undertaking.
 - e) Any item or picture of an item that can be considered to be or linked to extremist propaganda, including emblems and flags.
 - f) Any publication, audio, or video (including written translations) designed to sway individuals to violent extremism. Text documentation that could be deemed as weapons or armed/unarmed combat instructions.
 - g) Text documentation with instructions for manufacturing chemical or non-chemical explosive devices.
 - h) Any audio, video, or picture files that could be used to incite racial or religious hatred.
 - i) Any radical or extremist web sites, which propound racial or religious hatred, or magazines.
 - j) Any material that breaches Section 31 Crime and Disorder Act 1998: Racially or religiously aggravated public order offence.
- 9.2 Legal representatives and other agencies that may be disclosing material contained in this annex (**Annex C**) should be made aware that it should be sent separately to the A2DE Co-Ordinator in the establishment and marked accordingly so as not to cause harm or distress to any individual.
- 9.3 * Special arrangements to view such material in closed and secure conditions (i.e., visits booth) will be provided by arrangement and authority by A2DE staff.

10 A2DE Risk Factors

- 10.1 The default position of HMPPS is **READ ONLY** access. Allowing write access can pose a significant risk to security. File extensions can be amended, and system files manipulated. This would compromise the security measures put in place on the A2DE systems.

- 10.2 Illicit material could be created and sent under the cover of Rule 39. This would allow prisoners to write and run websites and or carry on with criminal IT based crime by proxy whilst in custody. Documentation used to radicalise or promote illegal activities could be produced.
- 10.3 USB ports and other expansion ports could be used to connect an illicit mobile phone providing the opportunity for uncontrolled communication in breach of Prison Rules.
- 10.4 USB and other memory storage devices containing information that could circumvent existing physical security measures, e.g., escape details, bomb-making information, photographs, can be brought undetected into prison through visits.
- 10.5 USB and other memory storage devices can be transferred between prisoners undetected in order to circumvent physical security measures.
- 10.6 The use of a USB dongle also called an Internet dongle is a small USB device that allows you to access the Internet. You can get both 3G and 4G dongles. It can be referred to as a dongle, USB modem, Internet stick, USB network adapter or USB mobile broadband stick. Dongles are popular because they offer greater flexibility and can be used on the go.
- 10.7 Integrated wireless capability could be used to access a wireless hotspot (i.e., a network connectivity point) outside the secure prison perimeter and control of the establishment, leading to the ability for a prisoner to communicate in an uncontrolled manner, in breach of Prison Rules. This would involve a close hotspot to be available.
- 10.8 Integrated wireless capability could be used to access a wireless hotspot within the establishment via a mobile phone leading to the ability to access the Internet.
- 10.9 Social media access. With the use of any of the connection methods full social media access would be available. Facebook, Instagram, Twitter etc. Live videos could be published using Periscope and similar applications and Direct Message requests for illicit items could be sent.

11 Summary of legal disclosure and Rule 39 material

- 11.1 In England and Wales, there are two main types of legal professional privilege. These are legal and litigation privilege. Any legally privileged material cannot be viewed on A2DE equipment. As listed below, three criteria will be examined to assess whether a communication and/or a document may be protected by legal professional privilege.
- 11.2 A communication and/or document (and its evidence) will be protected by privilege if it is:
 - a) Exchanged between a lawyer and a client (not including standard disclosure bundles).
 - b) Has remained confidential since its creation. It will remain privileged, despite having been disclosed to a third party since its creation, only if the disclosure was made on confidential terms and if the third party had, at the time of the disclosure, a common interest in the matter.
 - c) Relates to either: An existing, pending or reasonably contemplated litigation (this is litigation privilege). It is required to have been made for the dominant purpose of the litigation and related strategic legal advice.

Examples of this are:

- Correspondence between a defendant and their solicitor.
- Correspondence between a solicitor and their client.

- Instructions to a solicitor or legal team relating to the alleged case against the defendant.

11.3 These should be submitted within the standard Rule 39 policy directed by the Prisoner Communications Policy: PSI 49/2011.

Excludes internal grievance, disciplinary proceedings, fact finding inquiries and investigations; or legal advice given in a *contentious or non-contentious context (this is legal advice privilege).

It is required to have been made for the purpose of giving/obtaining legal advice. It will cover presentational or strategic advice provided that it relates to a client's legal rights and obligations. It will not apply to purely strategic or commercial advice.

All bona fide disclosure, which is disclosure submitted in open court by either the defence or prosecution, is NOT covered under Rule 39. Examples of this would be the Crown's case and submissions against the defendant. This can be checked against the disclosure bundle which should be obtained at the time of the application for A2DE equipment.

As all A2DE equipment is read only and does not have write ability enabled, it should be impossible for the defendant to claim any of the material on the equipment is covered by Rule 39. Some mistakenly think that the disclosure submitted (the paper or digital bundles from the CPS) are covered by Rule 39 as they are the legal claims made against the defendant. This is not the case. Disclosure is NOT covered by Rule 39.

** In general terms, contentious work includes areas where there is some sort of dispute that involves some adversarial process (whether or not this involves any sort of court or arbitration process) whereas non-contentious work does not.*

12 Searching of A2DE equipment

12.1 When staff undertake a cell search in line with the **Searching Policy Framework**, they are required to ensure that the A2DE equipment is intact and has not been tampered with (this includes checking the bag, power adapter, power cord and laptop). The equipment will be switched on and the CD DVD Rom drive, where applicable, ejected to enable staff to check for any hidden items.

12.2 If there is evidence to suggest the equipment has been tampered with the searching staff must seal the computer in its bag and then place it in a sealed property bag and inform the A2DE Coordinator/Team. The bag containing the computer will be passed to the A2DE Coordinator/Team for further inspection.

12.3 If inappropriate material is found on the equipment by the A2DE Coordinator/Team it must be placed in an Evidence bag and sealed pending further investigation by contacting Security.Procedures@justice.gov.uk and the prisoner placed on report.

12.4 The A2DE Coordinator will perform security checks at least once every three months in accordance with the **Annex E** on all A2DE equipment issued to prisoners. This is to ensure that the seals, hard drive, access to the equipment and the media are correct and have no inappropriate material on them. However, these security checks can be carried out by the A2DE Coordinator at any time.

- 12.5 If inappropriate material is found on the equipment it must be confiscated, placed in a bag, and sealed pending further investigation and the prisoner placed on report.
- 12.6 In the event that the prisoner fails to comply with this instruction, the prisoner is to be given a written warning, which will be kept on record. Any further breach of this instruction could result in confiscation of the equipment or a review of the conditions under which the machine can be accessed (see **Section 17 - Secure Condition** viewing would apply).
- 12.8 The in-cell equipment (laptop, bag, power adapter and power cord) are subject to search at any time by any member of staff in line with the **Searching Policy Framework**, this is especially important when defendants are taking the equipment to the authorised areas, such as legal visits, video link or court.

13 Procedure after A2DE equipment is removed

- 13.1 When a prisoners' case has concluded, and the Judge has either passed sentence or the defendant has been acquitted, the A2DE equipment is removed and purged locally by the holding prisons A2DE Coordinator to the DoD 35 standard for data erasure. (DoD 35 standard is a 3 pass delete/purge to Department of Defence standards during which the hard drive is safely purged so that previous prisoner's material cannot be accessed as it is permanently erased. This standard ensures that any previous material is irrecoverable).
- 13.2 Should the drive be faulty, this must be destroyed with accordance to the establishment ICT Destruction policy.
- 13.3 Once the equipment has been removed each system is checked for integrity and any illicit tampering by the holding establishment's A2DE Coordinators in accordance with the Prisoners compact (**Annex D1 & D2**).
- 13.4 All the data from each case which has been sifted at HMP Belmarsh, including any unused bundles, are stored on a secure network drive.
- 13.5 Should there be any appeal against conviction and one of the conditions at **4.15** is fulfilled, then as the original disclosure is already sifted, it can be re loaded onto A2DE equipment without causing any delays in the legal process along with any new evidence.

14 Legal teams handing in electronic documents via Court

- 14.1 There may also be occasions where the need to hand over a computer disc/ memory stick/ or hard drive arises for an A2DE registered prisoner. On such occasions the prisoners Legal Team is required to ask a member of prison staff for permission to hand over the computer disc in question. This situation should be unusual and, in order to maintain the integrity of the document set out above, permission may be refused unless a satisfactory explanation is provided. It should also be noted that the prisoner will not receive data contained on the disk until the necessary checks have been made by the A2DE Coordinator at the establishment. In the case of an on-going trial, this will not be before the next day's court business.
- 14.2 Where it is agreed by the Officer I/C of the escort that electronic media may be handed in, it is required to be handed in a sealed envelope with the following information annotated on the front of the envelope:
- a) Prisoner's name.
 - b) Prisoners number.

- c) Name of the solicitor depositing the item and name the firm to which they represent.
- d) Number and description of items being handed in.
- e) That's the Solicitor has confirmed in writing that the disc does not contain any legally privileged material and is not covered undertakings.

14.3 The escort contractor will pass the sealed envelope to the reception manager at the establishment who will be responsible for ensuring the sealed envelope is passed to the Orderly Office for secure storage until the A2DE team can collect it.

15 IT evidence received via the post

15.1 If it has been identified that there is disk contained within a letter covered by Rule 39, the letter must be opened in the presence of the prisoner and the disc returned to the solicitor to be sent into the prison in accordance with the procedures laid out above.

15.2 Only discs containing disclosure will be accepted by the prison. Any Rule 39 material should be loaded onto the solicitor's equipment for viewing with their client on their pre-booked legal visit.

16 Secure viewing of all Terrorism Act (TACT) cases

16.1 Justification and legal requirement to view material:

16.1.1 Under Article 6(3)(b), everyone charged with a criminal offence has the right to have adequate time and facilities for the preparation of his/her defence. Currently when the Crown disclose the bundles for court they are in their entirety. This means that inappropriate material (including but not limited, to beheadings, torture, acts of terrorism, extreme acts of violence) is included within the bundles.

16.1.2 ECHR Article 6 gives the prisoner the right to view what the Crown has submitted in its case. Currently the National A2DE Team at HMP Belmarsh sift through the files to find any inappropriate material and place it onto a secure read-only equipment to be viewed in a secure environment and not kept in possession. This reduces the risk of radicalisation. In TACT cases especially, a vast percentage of the files can be distressing to view.

16.2 How to manage the viewing:

16.2.1 Due to these risks all TACT disclosure should be deemed as secure and viewed only on a secure read-only equipment. As viewing is carried out in a secure area away from other prisoners the ability to use these files for acts of radicalisation or glorification are mitigated. **Please Note:** Prisoners are not allowed to take any notes made of a sensitive nature (as denoted under **Annex C** or by the CPS/ Court Order/ Police) whilst viewing the secure equipment back to their cells/wings.

16.3 How we define secure area:

16.3.1 A secure viewing area can be in a single cell over night during patrol state. This scenario should only be considered under extreme circumstances and only when all other options are exhausted. Audio/ video must not be played at a level that can be deemed as too loud by staff and this provision should be noted on a protocol log. The secure A2DE equipment must be removed from the prisoner's cell by staff before unlock and stored away securely. **A shared cell should never be treated as a secure viewing area** because of the risk of another prisoner either being radicalised or traumatised through exposure to violent material. In cell

phones need to be removed before allowing secure viewing. This accommodation must not have an in-cell telephone and the prisoner **must not** have access to another laptop/ computer at this time.

- 16.3.2 A separate secure environment away from other prisoners. For example, legal visits viewing area.
- 16.3.3 A prisoner will not be permitted to take their A2DE secure laptop to Court, Video link or on transfer.
- 16.3.4 Any other area that complies with the risk assessment for secure viewing (i.e., the inability for others to view the content).
- 16.3.5 Where the secure area that is used is an area other than the prisoner's cell, the prisoner is required to be given adequate time in that area to view the material. The length of time that is adequate will depend on a range of factors, including the volume and complexity of the disclosure material, and the characteristics of the prisoner (e.g., if they have learning disabilities/other educational needs). Should a prisoner raise concerns that they not have adequate time to review content a governor is required to ensure arrangements are put in place to accommodate their needs.
- 16.4 Staff must ensure that all **secure** equipment is removed when not being viewed in the secure area and is removed prior to the prisoner leaving the secure area, including the prisoner's own cell. This should be securely stored and returned to the prisoner if they request it during the next booked viewing session.
- 16.5 Should a TACT prisoner wish to make notes in preparation for discussion with their legal team, these notes cannot be removed from the secure viewing area by the prisoner and must be securely stored with the A2DE equipment in a sealed property bag. These will be returned and signed for on request only once the prisoner is in secure viewing conditions again.
- 16.6 If a TACT prisoner signs the **Annex H** before their sentencing date (where the equipment has been removed and the drive purged) and the CPS serve a paper sentencing bundle that is not voluminous and contains no sensitive material, the National A2DE Team at HMP Belmarsh will sift the material and issue the paperwork/forward to holding prison to issue to the prisoner.

17 Secure viewing of all non-Terrorism Act (TACT) cases

- 17.1 There may be times when approving a non-TACT case, the evidence may include some material of a sensitive nature that contravenes **Annex C**. The solicitor will be informed that their client can have all the material being served either loaded on a secure A2DE equipment to view in secure conditions for the duration of the trial or have an in cell A2DE equipment but view all sensitive material being served during booked legal consultations.

18 A2DE provided to another Government Agency

- 18.1 Whilst A2DE is primarily required for prisoners in HMPPS custody, this may not always be the case.
- 18.2 Where a request for A2DE equipment is received from another Government Agency each case needs to be suitably risk assessed and the appropriate justification provided.

- 18.3 Other Government Agencies who may apply for A2DE equipment include (this list is not exhaustive) – (**See Annex L**):
- a) Secure Children’s Homes who have a contract with the MOJ.
 - b) MoJ Secure Training Centres.
- 18.4 When a request is received by another government agency appropriate training will be provided to the required staff by HMP Belmarsh.
- 18.5 The named member of staff and SPoC from their SLT will be entered onto the “A2DE Contact Database – Live” (See **Section 19 - Auditable Recoding of all A2DE Staff & Equipment**).
- 18.6 Any agency requesting HMPPS A2DE equipment will need to ensure that the appropriate levels of security are in place as required within this policy and authorised by the appropriate HMPPS employed person from the Youth Custody Service (YCS).
- 18.7 In the event of a TACT/TACT connected or Counter Terrorism (CT) risk case, the regional CT must be consulted in any risk assessment process, who will check the security for the requested premises.
- 18.8 It may be necessary for an HMPPS member of staff to inspect (appropriate HMPPS employed person from the YCS) and advise the requesting agency in relation to security measure, storage, supervision, and record management.

19 Auditable recording of all A2DE staff and equipment

- 19.1 Every establishment working with A2DE will provide a Single Point of Contact (SPOC) from their Senior Leadership Team (See **Section 2.3 - Outcomes**).
- 19.2 Every establishment working with A2DE will provide suitable staff to be trained by the staff at HMP Belmarsh and afford them the time required to complete their work within this role (see Section 4.8 - Requirements).
- 19.3 Staff who have completed this training, along with the establishment SPOC will be entered on a Teams database channel, “A2DE Contact Database – Live”.
- 19.4 All A2DE equipment provide by HMP Belmarsh to establishments will be entered onto a Teams database channel, “A2DE Hardware Audit – Live”.
- 19.5 The A2DE Hardware Audit log will provide an ongoing list of all A2DE evidence equipment’s currently in use across the estate ensuring that those no longer in use are returned to HMP Belmarsh for future use.
- 19.6 If a prisoner is transferred the A2DE Hardware Audit log is required to be updated immediately to ensure that the equipment is appropriately tracked from the sending to the receiving establishment.
- 19.7 If the prisoner is transferred both the laptop/ drive and any paperwork/ case notes made by a TACT prisoner must be sent separately using a tracked service (Royal Mail) or by approved courier service only to the receiving establishment SPOC only.
- 19.8 Any losses of any A2DE equipment, files or records must be reported by the completion of an Incident Report Form and sent to: security@justice.gov.uk. Losses involving personal data should be reported to: dataprotection@justice.gov.uk

20 Records management for A2DE

- 20.1 Management of all A2DE records must be in line with **PSI 04/2018, Records, Information Management and Management Retention Policy.**
- 20.2 All official records held in both HMP Belmarsh and the establishment where the prisoner is located are required to be held in secure lockable cabinets with appropriate key security to those cabinets.
- 20.3 On completion of the A2DE process, all documentation held by the establishment where the prisoner is located pertaining to the A2DE record will be filed in the prisoner's core record as evidence of compliance with process.
- 20.4 All duplicated A2DE records held at HMP Belmarsh should be retained only for the length of the period that would ensure that further requests and appeals would not require the recommencement of the application process. This should be to a maximum of 2 years.
- 20.5 Any duplicated records held at HMP Belmarsh can be securely destroyed without entering onto a destruction log as these are duplicates of those held in the establishments where the prison is located.



APPLICATION FOR A2DE EQUIPMENT

NAME:	No:	COURT DATE:	LOC:
--------------	------------	--------------------	-------------

Issue of A2DE equipment is on a case-by-case basis. Below is an example of some of the application criteria.

1. The evidence in your case has been submitted by the Crown in electronic format and is too voluminous (minimum 3500 pages of evidence, excluding CCTV & audio evidence) to be viewed in paper format or during a legal visit.
2. The defence is complex or requires the investigation of data that could not easily be carried out without the use of the equipment provided.
3. You have a particular disability, or there are other relevant health factors.

Please give details of your particular needs for an A2DE equipment
(Attach additional sheets if required)

The application **will not** be considered and **not** approved if: -

4. You wish to type letters to your legal team rather than write them by hand for your trial or personal defence.
5. If you want the equipment to appeal against sentencing.
6. If you would not be competent to use the equipment provided.
7. If you require the equipment in order to prepare your appeal application to the court.

Please provide details of why this cannot be viewed during a legal visit with your legal representative.

Do you have you any medical conditions that should be considered?

How long do you think this legal work will take?

All disclosure material will be loaded onto the data partition on the issued A2DE equipment.
If disclosure not covered by Rule 39, there will be no breach of Prison Rule 39 in its entirety.

Please provide full contact details of your legal representative, including telephone number and email address.

Address: _____ Telephone: _____

_____ Email: _____

Post Code: _____

Prisoner's Signature.....

Date.....



Response to Prisoner Application for Use of A2DE Equipment

<u>NAME</u>	<u>PRISON NUMBER</u>	<u>LOCATION</u>

Your application to have A2DE has been considered.

Has the application been approved?

- ✓ YES/NO - NON-SECURE (In Possession)
- ✓ YES/NO - SECURE

Your application has been approved from initially then subject to reviews every 3 months.

Reason for Decision:

Additional Information:

Non-sensitive material can still be sent directly to you via post, providing it is not of a secure nature and does not contravene the **ANNEX C**.

Please be aware that if you are in possession of any material that contravenes the **ANNEX C** (included with this letter) it is your responsibility to inform staff immediately. You can also send a general application to the Access to Digital Evidence department to inform us.

Your solicitor has been informed in writing of our decision.

Name: A2DE COORDINATOR		Date	
-------------------------------------	--	-------------	--



Response to Prisoner Application for Secure Use of A2DE (TACT)

<u>NAME</u>	<u>PRISON NUMBER</u>	<u>LOCATION</u>

Your application to have A2DE has been considered.

Has the application been approved?

✓ YES/NO – SECURE

Your application has been approved from initially then subject to reviews every 3 months.

Reason for Decision:

Access to Digital Evidence Policy Framework dictates that as a defendant facing TACT offences any and all disclosure served in your case is to be considered secure material.

As per Access to Digital Evidence Policy Framework you have been granted the use of Secure equipment only.

The Access to Digital Evidence coordinator will fully explain the process and issue you with the relevant paperwork.

Any notes taken in preparation for discussion with your legal team will be securely stored in a sealed property bag with the A2DE equipment and returned, and signed for, on request only once you in secure viewing conditions again.

Additional Information:

You will not be permitted to take this secure equipment to Video Link or Court, nor will you be able to take the equipment should you transfer to another establishment.

Non-sensitive material can still be sent directly to you via post, providing it is not of a secure nature and does not contravene the **ANNEX C**.

Please be aware that if you are in possession of any material that contravenes the **ANNEX C** (included with this letter) it is your responsibility to inform staff immediately. You can also send a general application to the Access to Digital Evidence department to inform us.

Your solicitor has been informed in writing of our decision.

Name: A2DE COORDINATOR		Date	
---------------------------------------	--	-------------	--



Inappropriate Material

No Material listed below should be allowed in possession and secure viewing protocols should be used to view such material.

- Video, audio or picture files, containing or depicting any violent act that appears to glorify acts of Terrorism. For example, suicide bombings or executions, audio by any radical preacher, cleric or any radical audio from any religious denomination.
- Video, audio or picture files containing or depicting any violent act that appears to glorify acts of extreme violence, this could include Gang Culture video's (known as Drill Video's).
- Video, audio or picture files of a graphic nature (Graphic material is defined as any material that may cause alarm, distress or harm to any individual that is exposed to the content).
- Any material subject to a signed legal undertaking by the legal representative (i.e., sensitive evidence required to be handled appropriately).
- Any item that can be considered to be or linked to extremist propaganda, including emblems and flags.
- Any publication, audio or video (Including written translations) designed to sway individuals to violent extremism.
- Text documentation that could be deemed as weapons or armed/unarmed combat instructions.
- Text documentation with instructions for manufacturing chemical or non-chemical explosive devices.
- Any radical or extremist web sites, audio, video or picture files, which propound racial or religious hatred, or magazines.
- Any material that breaches Section 31 Crime and Disorder act 1998: - Racially or religiously aggravated public order offence.
- Text documentation containing any material of a sexual nature, or describing or depicting any sexual act.

Legal representatives and other agencies that may be disclosing material contained in this annex should be made aware that it should be sent separately to the Access to Digital Evidence Co-Ordinator in the establishment and marked accordingly so as not to cause harm or distress to any individual.

No Material listed below will be permitted to be loaded to A2DE equipment at any time.

- Video, audio or picture files containing any material of a sexual nature, or depicting any sexual act.
- Any file deemed as a security risk, such as:
 - Encrypted files
 - A file that has password protection be it compressed or uncompressed.
 - Any file that has had its file extension altered.
- Any file that could contain a possible virus.
- Any application or programme licensed or otherwise unless supplied as a bespoke player for material.
- Any executable file. (i.e.- a file that could be run or started by clicking the icon) unless supplied as a bespoke player for material.
- A file that has password protection be it compressed or uncompressed.
- Any operating system or system files that could be collated to form an operating system.
- Hardware or software device drivers.
- Any software that could be used to alter or gain access to the operating system.

- **You are not permitted to make or have in-possession, in cell or in any other area of the prison any notes/annotations of a secure nature (contravenes this document) made during the course of your secure viewing.**



COMPACT FOR THE USE OF IN-CELL (In Possession) A2DE EQUIPMENT

Having considered the application of **NAME AND NUMBER** for **In Cell** A2DE equipment, the items listed below will be supplied under the terms of this compact for legal relating to a criminal case only.

The equipment will consist of:

- | | |
|--------------------------|-----------------------|
| 1. 1 X A2DE LAPTOP | Serial No: xxxxxxxxxx |
| 2. 1 X MAINS TRANSFORMER | |
| 3. 1 X POWER LEAD | |
| 4. 1 X LATOP BAG | |

Equipment will be provided for in cell use only. The equipment may not be taken on the exercise yard, on association, in any other prisoner's cell, loan to any co-defendants or when the prisoner is engaging in other activities. This equipment may be taken to Court, Legal Visits/Video Link and used solely by the prisoner for the duration of the legal visits.

The equipment will be provided from the date of:

This is subject to an initial period of 3 months and then 3 monthly reviews.

Prison No :	XXXXXX	Name :	XXXXXX
LOGIN :	USER	PASSWORD :	XXXXXX

Agrees to abide by the following terms and conditions:

- Will only use the issued equipment for the purpose of viewing legal disclosure.
- Will not loan or allow access of the A2DE equipment to any other prisoner.
- You are solely responsible for the items listed above. If you have wilfully damaged the A2DE equipment you will be placed on report for the wilful damage of prison property and may be liable for the cost of the machine. Any tampering or loss of the equipment will be treated as a breach of this compact and as such a formal warning will be issued which could result in the withdrawal of the equipment or a review of the conditions that the equipment may be viewed in (secure conditions).
- Accidental damage to A2DE equipment must be reported to the houseblock staff and you must also send notice in writing to the A2DE department informing them of the accidental damage within 24 hours. Failure to do so will be treated as a breach of this compact and as such a formal warning will be issued which could result in the withdrawal of the equipment or a review of the conditions that the equipment may be viewed in (secure conditions).
- Will immediately bring to the attention of the A2DE Coordinator or prison staff any operating difficulties encountered.
- Any files that are deleted accidentally or otherwise modified will not be recoverable by the establishment.
- You are not permitted to make changes to the file structure, copy, and move, rename, or create any new files. All information contained on the equipment must have been submitted by the CPS/SOLICITOR/POLICE as disclosure.
- Disclosure material will have files loaded to the designated section of the equipment.

- Will not access or make any attempt to access the operating system or operating system partition.
- Will not install or attempt to install any programmes or applications on the equipment. Failure to comply may result in the removal of the equipment.
- Will comply with the rules regarding prisoner communications and will not circumvent or attempt to circumvent the procedures.
- Will allow the A2DE Coordinator to take the equipment away without notice to load new evidence and to routinely scan the hard drive of the equipment for any inappropriate material or viruses at any time.
- Will not have in possession any **evidential** disks that contain any computer data, illicit or inappropriate material.
- Will not share (physical or audio) or let any other prisoner use the equipment issued above.
- Will not play any audio or video containing audio at a level that can be deemed as too loud by staff.
- Will not remove the equipment from your accommodation unless it is for the purpose of a booked legal consultation, video link appearance or court appearance.
- Will hand over the A2DE equipment to staff if getting transferred to another prison or getting released.
- Will immediately hand over any and all A2DE equipment upon request by a member of staff.
- Has been made aware of the health and safety issues relevant to the use of IT equipment (*see below*).

Monitor: The monitor/screen should be positioned about 18 to 20 inches from your eyes and the top of the screen should be at eye level or lower. Ensure the monitor/screen is positioned to prevent reflected glare from windows or lights.

Posture: Sit with your back relaxed and your hips and knees at an approximate 90° angle to your chair's seat and your thighs roughly parallel to the floor. Keep your feet flat on the floor.

Mouse: If using a mouse, move your entire arm instead of just bending your wrist. Ensure the mouse is positioned for ease of movement.

Breaks: If working for long periods, take regular breaks. Get up from your chair, stretch and loosen your wrists with gentle exercise. Do not sit in one position for long periods.

- Failure to comply with the conditions outlined in this compact (as per PSI 2/2001) or any local policy may result in withdrawal of the IT facility or restricted use of A2DE equipment.
- The Hard drive will be purged when a prisoner has been acquitted/ convicted and sentenced or has signed the Annex H
- If headphones are required for use, these should be purchased by the prisoner in line with local facilities policy (Exceptions overriding such policy on approval from The Governor)
- I accept these items on loan from the prison service and will comply with all regulations appertaining to the use of the equipment.
- Once the judge has passed sentence, you have been acquitted or you have signed the Annex H the equipment will immediately be removed, your A2DE application will be closed, and the equipment purged.

Signed..... Name..... Date.....
Prisoner

Signed..... Name..... Date.....
Establishment



COMPACT FOR THE USE OF SECURE A2DE EQUIPMENT

Having considered the application of **NAME & NUMBER** for A2DE **Secure** equipment, the items listed below will be supplied under the terms of this compact for legal relating to a criminal case only.

The equipment will consist of:

1. 1 X A2DE SECURE LAPTOP
2. 1 X MAINS TRANSFORMER
3. 1 X POWER LEAD
4. 1 X LAPTOP BAG

Serial No:

Equipment will be provided for **SECURE VIEWING ONLY**. Secure viewing laptops are for restricted supervised use in a secure environment only. This laptop can NOT leave the establishment, can NOT be issued for use at Video Link, Court or on Transfer. The machine can be requested by the prisoner to view with their legal team during a booked legal consultation.

The equipment will be provided from the date of:

This is subject to an initial period of 3 months and then 3 monthly reviews.

Prison No :

Name :

LOGIN :

PASSWORD :

Agrees to abide by the following terms and conditions:

- Will only use the issued equipment for the purpose of viewing legal disclosure.
- **Will not make or have in-possession, in cell or in any other area of the prison any notes/annotations of a secure nature (contravenes Annex C) made during the course of your secure viewing.**
- Any notes taken in preparation for discussion with your legal team will be securely stored in a sealed property bag with the A2DE equipment and returned, and signed for, on request only once you in secure viewing conditions again.
- You are solely responsible for the items listed above. If you have wilfully damaged the A2DE equipment you will be placed on report for the wilful damage of prison property and may be liable for the cost of the machine. Any tampering or loss of the equipment will be treated as a breach of this compact and as such a formal warning will be issued which could result in the withdrawal of the equipment.
- Accidental damage to A2DE equipment must be reported to staff and you must also send notice in writing to the A2DE department informing them of the accidental damage within 24 hours. Failure to do so will be treated as a breach of this compact and as such a formal warning will be issued which could result in the withdrawal of the equipment.
- Will immediately bring to the attention of the A2DE Coordinator or prison staff any operating difficulties encountered.
- Any files that are deleted accidentally or otherwise modified will not be recoverable by the establishment.

- You are not permitted to make changes to the file structure, copy, and move, rename, or create any new files. All information contained on the equipment must have been submitted by the CPS/SOLICITOR as disclosure.
- Disclosure material will have files loaded to the designated section of the equipment.
- Will not access or make any attempt to access the operating system or operating system partition.
- Will not install or attempt to install any programmes or applications on the equipment. Failure to comply may result in the removal of the equipment.
- Will comply with the rules regarding prisoner communications and will not circumvent or attempt to circumvent the procedures.
- Will allow the A2DE Coordinator to take the equipment away without notice at any time to load evidence and to routinely scan the hard drive of the equipment for any inappropriate material or viruses at any time.
- Will not have in possession any **evidential** disks that contain any computer data, illicit or inappropriate material.
- Will not share (Physical or Audio) or let any other prisoner use the equipment issued above.
- Will not play any audio or video containing audio at a level that can be deemed too loud by staff.
- Will not remove the equipment from **the secure environment**.
- Will immediately hand over any and all A2DE equipment upon request by a member of staff.
- Has been made aware of the health and safety issues relevant to the use of IT equipment (*see below*).
Points to note when using IT equipment.

Monitor: The monitor/screen should be positioned about 18 to 20 inches from your eyes and the top of the screen should be at eye level or lower. Ensure the monitor/screen is positioned to prevent reflected glare from windows or lights.

Posture: Sit with your back relaxed and your hips and knees at an approximate 90° angle to your chair's seat and your thighs roughly parallel to the floor. Keep your feet flat on the floor.

Mouse: If using a mouse, move your entire arm instead of just bending your wrist. Ensure the mouse is positioned for ease of movement.

Breaks: If working for long periods, take regular breaks. Get up from your chair, stretch and loosen your wrists with gentle exercise. Do not sit in one position for long periods.

- Failure to comply with the conditions outlined in this compact (as per PSI 2/2001) or any local policy may result in withdrawal of the IT facility or restricted use of A2DE equipment.
- The Hard drive will be purged when a prisoner has been acquitted/ convicted and sentenced or has signed the Annex H
- If headphones are required for use, these should be purchased by the prisoner in line with local facilities policy (Exceptions overriding such policy on approval from The Governor)
- I will not take the equipment on transfer or court and will hand it over to staff immediately upon request.
- I accept these items on loan from the prison service and will comply with all regulations appertaining to the use of the equipment.
- Once the judge has passed sentence, you have been acquitted or you have signed the Annex H the laptop will immediately be removed, your A2DE application will be closed, and the laptop purged.

Signed.....
Prisoner

Name.....

Date.....

Signed.....
Establishment

Name.....

Date.....

This compact supersedes all previously signed compact



A2DE INVENTORY/SECURITY CHECKS

Name:		Number:		Location:	
Make/Model		Equipment Number:	Serial		
Issued by:		Date:		Sign:	

Security Checks

	Initial issue Initial checks completed on setup	Date	Date	Date	Date	Date
Equipment Serial Number						
Carry case						
Hard Drive (HDD) Check						
Name						
Signature						
HDD Purge Date		HDD Purge Name		HDD Purge Signature		

Virus checks will be carried out upon receipt of material by the National A2DE Team at HMP Belmarsh
(These checks must be completed once within a 3-month period of issue)



COMPACT FOR THE USE OF A2DE EQUIPMENT REVIEW

PRISONER NAME	PRISONER NUMBER

The continued use of the A2DE facility has been reviewed and it is agreed that the equipment can be used for a further period of 3 months, as dated below.

From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----
From: __ / __ / __ Name: -----	Ending: __ / __ / __ Signature: -----



Refusal of A2DE Assistance

Date:

I confirm that I do not require assistance nor the use of the A2DE facility offered the purpose of which has been fully explained to me.

I acknowledge that by refusing this assistance I will have to view my evidence on a booked legal consultation with my legal team or have it provided in paper format, providing that it does not breach prison security or contain any disclosure that would be subject to ANNEX C contained in the prisons Local Operation Procedure.

I am fully aware that I am **PROHIBITED** from being in possession of any evidence that contravenes the Annex C (enclosed with this letter)

Signed: Name: Date:
Prisoner

Signed: Name: Date:
A2DE coordinator

Should a prisoner not wish to engage with the A2DE coordinator and refuse to sign this document the A2DE coordinator may complete the below section and have it signed by an independent witness.

<u>NAME</u>	<u>PRISON NUMBER</u>	<u>Location</u>

Has refused to engage with the A2DE process and therefore is ineligible for A2DE assistance, no further action will be taken.

Signed: Name: Date:
A2DE Coordinator

Signed: Name: Date:
Independent Witness



Confirmation of removal of A2DE equipment

I confirm that I no longer require the use of the A2DE equipment that has been provided to me.

I acknowledge that the equipment has been removed on by an A2DE member of staff.

By signing this document, I understand that my A2DE application will be fully closed, the equipment will be removed (no further access in the case of secure equipment) and its hard drive will be purged of all data.

Any further material served in my case or for sentencing will now need to be sent to me directly in paper format via the postal system providing it does not contravene the ANNEX C, I can also continue to view material with my solicitors during a booked legal visit.

Reason for removal:

Signed.....
Prisoner

Name.....

Date.....

Signed.....
Establishment

Name.....

Date.....

Risk Assessment for Secure Viewing (EXAMPLE)

Risk	Who is affected	Key Risk Factors	Control Measures	Review
<p>Unauthorised viewing/sharing of secure TACT material, which is designed to glorify acts of terrorism and has the potential to radicalise.</p> <p>Unauthorised viewing/sharing of other types of sensitive material including pornography, sexual abuse, violence, which may be protected by a legal undertaking, although not always so</p> <p>NB This covers the risk of material being shared both with others in the prison and being put onto social media sites or sent out of the prison – possibly with use of illicit mobile phones.</p>	Staff and Prisoners	<p>Staff and prisoners subjected to graphic and violent images and videos including torture, beheadings, and similar acts of atrocity.</p> <p>Prisoners having the opportunity to exult in material that glorifies violence and/or acts of terrorism, potentially leading to radicalisation, or as a minimum impeding rehabilitation.</p> <p>Reputational damage to the prison, HMPPS and the Government.</p>	<p>All secure viewing is to be carried out in a controlled environment. Secure material will be marked 'SECURE' and should be treated as such.</p> <p>Secure material will be clearly labelled, and access will only be provided on the appropriate A2DE equipment, which must not be permitted outside the "controlled environment".</p> <p>A Controlled environment is deemed as an area that:</p> <ul style="list-style-type: none"> • Cannot be overlooked by other prisoners. • Will not play any audio or video at a level that can be deemed too loud by staff. • The area must have a secure lockable door. • Equipment must never be allowed in possession outside of the secure area. • A plug point must be accessible for the power supply. • A suitable chair and table should be provided. 	All local risk assessments, safe systems of work and security strategies will be reviewed regularly or when circumstances significantly change.

			<ul style="list-style-type: none">• Pen and paper for note taking and annotations should be made available.• The prisoner must not take any notes of a secure nature back to their cell/ wing/ houseblock that contravenes Annex C, and any notes taken must be stored securely in a sealed property bag in an appropriate safe area and signed for before being reissued with A2DE equipment.• The equipment must be securely stored in an appropriate safe area when not in use.• Staff may not view the material on the equipment as it can be highly sensitive, distressing and or subject to a legal undertaking.• The prisoner is required to sign each time they view the material including both date and time.	
--	--	--	--	--

Role of A2DE Co-Ordinator

Each prison establishment will appoint a Single Point of Contact for A2DE from their Senior Leadership Team who will ensure that the Co-ordinator, once trained by the National A2DE Team at HMP Belmarsh, is afforded the facility time to complete their work.

1. The A2DE Coordinator will ensure that A2DE equipment is used only for the legal purpose issued, that only licensed copies of software are being used and that other files on the computer, storage drives, and any media supplied by legal representatives/the Crown Prosecution Service (CPS) do not contain inappropriate, illegal material or viruses.
2. When the A2DE Coordinator receives a general application from a prisoner they are required to check that the prisoner is on remand and not sentenced.
3. The A2DE Coordinator is required to then send an Annex A to the prisoner and inform them they need to complete and return the form to their office within 14 days. If after 14 days, the prisoner has not responded a further Annex A should be sent allowing a further 7 days. Should the prisoner then fail to fulfil the request the application should be closed. The A2DE audit requires that applications be processed, considered and answered in a timely manner.
4. Once the A2DE Coordinator receives the completed Annex A, it is required to be checked to ensure all sections have been filled in and signed by the prisoner. The A2DE coordinator is required to check the prisoners' charges and any security alerts on NOMIS and provide this information to the National A2DE team at HMP Belmarsh.
5. The A2DE Coordinator is responsible for emailing the Annex A including the relevant information (alerts/charges) to the National A2DE Team at HMP Belmarsh .
6. Once the completed Annex A has been received by the National A2DE Team at HMP Belmarsh they will contact the prisoner's legal team in writing, requesting all documentation and evidence served to date to decide if the prisoner fits the criteria.
7. The National A2DE Belmarsh Team are responsible for the receiving of material, sifting and decision making of any and all A2DE applications.
8. Local A2DE coordinators are not permitted to sift or make decisions on A2DE applications unless explicitly requested to do so by the National A2DE Belmarsh / Security Procedures.
9. Once the application has been considered by National A2DE Belmarsh Team an Annex B either approving or declining the application will be provided to local A2DE coordinators to be issued the prisoner.
 - a) If the application is successful the local A2DE coordinators will prepare equipment, load the evidence, generate the prisoner Annex D to be issued to the prisoner.
 - b) The A2DE Coordinator is required to send a copy of the signed Annex D to the National A2DE Belmarsh Team and return the material (USB/Drive or Discs) back to the asset owner (Solicitor/CPS/Police/National A2DE Belmarsh Team). A folder is required to be opened and all paperwork relating to this application stored within for audit purposes.
 - c) Should the application be unsuccessful and declined the prisoner should be issued with the appropriate Annex B and the application closed.

- d) The National A2DE Belmarsh Team is responsible for informing solicitors of their clients A2DE applications outcome in paper.
10. Files on the equipment must not be encrypted, password protected or hidden from view, if the prisoner has failed to comply with this instruction. They will be given a written warning, which will be kept on record.
 11. Any further breach of this instruction could result in confiscation of the equipment.
 12. A separate stand-alone computer with up-to-date virus software installed will be used to scan for viruses, illicit or inappropriate material and hidden or encrypted files before being transferred to the prisoners A2DE equipment.
 13. Where a virus or corrupted disk is detected, the A2DE Coordinator will return the disk to the legal representative or CPS and request a non- infected / corrupted copy of the material. A covering letter will be attached with the disk.
 14. Rule 39 correspondence from the prisoner to their legal advisors and/or the court must be hand-written or typed on a typewriter.
 15. All HMPPS specification A2DE equipment will have an administrators account for use by the IT Manager / A2DE Coordinator or their deputy.
 16. All HMPPS specifications computers will be etched with an individual serial number.
 17. HMPPS issue equipment is required to be recorded on the prisoners in possession property card and endorsed "not to go on transfer with prisoner" by the A2DE Coordinator.
 18. The A2DE Coordinator will co-ordinate all relevant documentation and keep accurate records for reference / audits. This includes maintaining a log when the laptop is provided to the prisoner in secure viewing conditions.
 19. A scanner, printer or printing facilities will not be provided at any time for the purpose of A2DE.

A2DE HMP Belmarsh Process Map



