Data Sharing Agreement

For the necessary sharing of data between Durham University and St Chad's College, Durham (the Parties)

This agreement is necessary for the parties to deliver and manage the university education, college membership, accommodation and welfare support of registered students of Durham University who are members of St Chad's College. It is also necessary for the parties to manage the relationship between the parties and those people who are alumni of both institutions. The agreement is also intended to ensure compliance with the Data Protection Act 1998, the General Data Protection Regulation, and the Data Protection Act 2018 by both parties.

The relationship between the parties is governed by a memorandum of understanding available here: https://www.stchads.ac.uk/about/documents/ This memorandum sets out the arrangements under which St Chad's College provides a service to Durham University together with the ways in which the parties relate to one another. The memorandum requires the parties to enter into a data sharing agreement.

The purpose of this agreement is to ensure that, as far as possible, St Chad's College and Durham University can exchange data in the same way that the maintained Colleges exchange data with the University (and University-managed professional services). Data will be shared or exchanged in accordance with published policies, standard procedures and established practice.

St Chad's College has adopted the data protection, records management and information security policies of Durham University (as amended from time to time) – see the University's information governance pages for details: https://www.dur.ac.uk/ig/ The College stores data on University servers and buys in IT services from the University.

This Agreement commences when it is signed and dated by both parties and will continue (unless terminated early) for five years. It is expected that after five years a new agreement will be entered into. The agreement will be reviewed annually to ensure compliance with relevant legislation and best practice.

Data will be shared in accordance with the detailed provisions that follow.

1 Basis for sharing and processing

Both parties are data controllers. Data is being transferred as part of the arrangements between them set out in the Memorandum of Understanding.

The parties will routinely share personal data for purposes of departmental administration, and academic progress and attendance monitoring (including all information held on the University's academic database – Banner – which is to be regarded as a shared data pool). The types of data collected will be detailed in the parties' privacy notices.

The lawful basis for this processing is that it is necessary for the contracts we have with the individual data subject. The University and College need to process information in order to deliver the agreed services to students.

Where appropriate, and in relation to particular students, the parties may share special category data (sensitive personal data) in relation to concessions, appeals, Self-Certification of Absence forms, Serious Adverse Circumstances forms, student visa applications, and complaints, and for the purpose of implementing published University policies on Discipline, Mental Health, Sexual Violence and Misconduct, Disability, Fitness to Study and other policies which may be introduced from time to time. Again, again, the types of data collected will be detailed in the parties' privacy notices.

The lawful basis for this processing under Article 6 of GDPR is "contract" as above. The condition for processing special category data under Article 9 is that it is carried out in the course of the parties' legitimate activities and with appropriate safeguards.

The parties will routinely share personal data about alumni for the purposes of alumni relations and fundraising (including all the information relating to alumni of St Chad's College – who are also alumni of the University – held on the University's alumni database Raiser's Edge which is to be regarded as a shared data pool).

The lawful basis for this processing will be legitimate interest and, in some cases, consent.

2 General

For the purposes of this Agreement the parties acknowledge that both parties are data controllers and both parties will perform their obligations under the Agreement in accordance with the requirements of the Memorandum of Understanding, the Data Protection Act and GDPR, and solely for the purposes set out in this Agreement.

3 Security

Both parties will implement and maintain appropriate technical and organisational measures to safeguard the personal data against unlawful and unauthorised processing of the personal data and against accidental loss, destruction of and/or damage to the personal data. In particular, both parties:

a. keep the personal data strictly private and confidential including encryption or pseudonymisation of personal data where appropriate;

b. prevent absolutely any unauthorised disclosures of personal data and minimise any authorised disclosure of the personal data to third parties to the fullest extent possible;

c. allow access to the personal data strictly on a 'need to know' basis and use appropriate access controls to ensure this requirement is satisfied;

d. ensure that any recipients of the personal data are subject to a binding duty of confidentiality in relation to the data;

e. ensure they have the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

f. maintain a record of their processing activities under or in connection with the Agreement in accordance with Article 30 of the GDPR and make such record available to the relevant supervisory authority upon request;

g. put in place and maintain the security measures set out in the schedule to this Agreement.

The college will make use of University IT systems and data storage under the terms of the service agreement.

3.1 The parties' will retain the data only for such period as is necessary for the performance of the Services. Data will be retained and deleted in accordance with the University's published data retention schedules.

3.2 However, neither party will destroy information without first informing the other party.

4 Database rights (to be amended)

You acknowledge that you are processing the personal data as a service provider and data processor and that, as between the parties, the personal data and all intellectual property rights in the personal data shall belong to us absolutely.
To the extent that any intellectual property rights in the personal data vest in you (whether by operation of law or otherwise), you assign (and shall procure that any of your agents and subcontractors shall assign) absolutely with full title guarantee all your rights, title and interest (if any) in respect of the personal data and the intellectual property rights in and to the personal data with the intent that such property and intellectual property rights shall, if they are in existence, immediately vest in us and shall, if they are yet to come into existence, vest in us immediately upon the same coming into existence.
We grant you a royalty-free licence during the term of this Agreement to use, copy and store the personal data solely for the purposes of performing and fulfilling your rights and obligations under this Letter (but for no other purpose).

5 Personnel

Both parties will take reasonable steps to ensure the reliability of all personnel (whether employees, volunteers, contractors or otherwise) that may have access to the personal data and to ensure that they are adequately trained in the good handling of personal data and are subject to a duty of confidentiality.

6 Processing

Both parties will process data only in accordance with published policies, standard procedures and established practice; and will not use the personal data for any purpose other than those set out in this Agreement.

7 Third Party Data Processing

If either party subcontracts activities that will involve a third party processing the personal data they will remain fully liable for the acts and omissions of any third party.
If either party engages a third party to process personal data, they will:

a. only choose a third party who will provide sufficient guarantees regarding the security measures it is required to take for the processing of the personal data which shall at least be equivalent to those measures that are required under the

terms of this Agreement; and will take reasonable steps to ensure the third party's compliance with those measures.

b. ensure that the processing is carried out under a written contract;
c. require the third party to comply with the same obligations in this Agreement that apply to them as if the third party were in their place.

8 Transferring personal data outside the European Economic Area

Neither party will transfer or permit the transfer of personal data to any territory outside the European Economic Area without ensuring that the transfer is subject to adequate security measures and is in accordance with Information Commissioner's Office guidelines

9 Providing assistance

The parties will assist each other promptly with all requests which may be received from individuals in order that they may comply with their obligations and fulfil the rights of data subjects under the Act and GDPR, including:

a. responding to requests or queries from data subjects in respect of their personal data;
b. cooperating with an investigation in connection with the personal data by a regulatory body; or
c. reconstructing and/or otherwise safeguarding the personal data,

within a reasonable period of time.

The parties will notify each other promptly (and in any event within two business days of receipt) of any complaint, an exercise of a right under section 7 of the Act or Articles 15 to 18 (inclusive) or 20 to 22 (inclusive) of the GDPR (as applicable) or other request (such as from any applicable government, agency or regulator) in respect of personal data except where doing so would breach applicable law.

The parties will notify each other without undue delay (and in any event within 48 hours) if you become aware or suspect a personal data breach. For these purposes a breach includes (but is not limited to) sending personal data to a wrong recipient, systems going down so that personal data is inaccessible or data becomes corrupted, or accidently deleted. The notification shall include the nature of the personal data breach, the likely consequence of such breach and the categories and approximate number of data subjects concerned. Neither party will enter into communications with

anyone about any suspected data breach until the matter has been discussed by both parties.

10 Indemnity

Each party shall indemnify the other against any costs, claims, expenses (including reasonable legal costs) damages, liabilities, actions and proceedings brought against such other by any third party arising out of a breach of this Agreement by the indemnifying party (or an employee, agent or subcontractor of such party).

In particular, the University will also indemnify the College against such costs if the data breach is the result of a hardware failure or a security breach on the University's IT systems.

11 Record Keeping and Audit

Both parties will:

a. maintain a record of the processing activities which relate to the Agreement in accordance with the requirements of Article 30(2) of the GDPR; and
b. maintain such records as are required by paragraph 3(g) of this Agreement.

Each party will permit the other to monitor their compliance with the terms of this Agreement which may involve them or their nominated representative coming onto any premises where the personal data are being stored or processed and having access to all systems and files used for processing the personal data. They will provide each other with any information necessary for the audit upon request.

12 Ending this arrangement

A data sharing agreement is required by the Memorandum of Understanding between Durham University and St Chad's College and this Agreement must therefore be renewed when it expires.
Notwithstanding the above, either party may end this arrangement by giving three months' written notice to the other. This notice period will be reduced so that it ends with immediate effect if the reason for ending the arrangement is because:

1. a resolution is passed or an order is made for either party to be wound up (other than for a solvent amalgamation or reconstruction);
2. the other becomes subject to an administration order or a receiver or administrative receiver is appointed;

3. somebody with a right to do so takes possession of any of the other's property or assets in the event of it being dissolved; or
4. the other ceases to carry on business in the United Kingdom.

In addition, either party will be entitled to end this arrangement immediately on written notice if the other party does, or fails to do, something that they are obliged to do which compromises the personal data or causes either party to violate the Act, (as applicable) the GDPR and any other relevant data protection laws.

13 General

Each party will do and execute and/or arrange for the doing and executing of, any act and/or document reasonably requested of it by any other party to implement and give full effect to the terms of this Agreement.

This arrangement is personal to the parties and neither party is permitted to assign or transfer any of their rights or obligations in it without the written consent of the other.

The parties are entering into this arrangement for the benefit of themselves and the individuals whose personal data is stored and processed - either party, and any data subject, will be entitled to enforce it. Other than that, no other person will have any enforceable rights under this arrangement and the Contracts (Rights of Third Parties) Act 1999 will not apply.

The parties may amend this arrangement by written agreement between them without needing the consent of any other person.

This Agreement and the arrangement made under it are governed by and will be interpreted in accordance with English law. In the event of a dispute, the parties agree that the English courts will have non-exclusive jurisdiction to hear the case.

Signed for and on behalf of Durham University

Signature: .....
(authorised signatory)

Print name: .....

Position……..

Date: .....

Signed for and on behalf of St Chad's College

Signature: .....
(authorised signatory)

Print name: .....

Position……..

Date: .....

Schedule - Security Measures

1 Definitions

The following definitions apply to this schedule:

Agreement	means this agreement (of which this schedule forms part), together with all other of its Schedules, annexures and all documents that are incorporated into any of them whether by inclusion or reference
Personal Data	means personal data (having the meaning ascribed under the Data Protection Act 1998 or (as applicable) the General Data Protection Regulation)
Processing	has the meaning ascribed under the Data Protection Act 1998 or (as applicable) the General Data Protection Regulation and the terms 'Process' and 'Processed' shall be construed accordingly
University Personnel	means any person that is used by, or on behalf of, Durham University and who may have access to the Personal Data
College Personnel	means any person that is used by, or on behalf of, St Chad's College and who may have access to the Personal Data

2 GENERAL OBLIGATIONS

When Processing Personal Data in the course of performing their obligations and exercising their rights under, or in connection with, this Letter, the University and College shall, and shall procure that University Personnel and College Personnel shall, as a minimum, comply with the measures set out in this Schedule to protect the Personal Data.

MANAGEMENT

1	**Security management**	The University and College will ensure that senior management of the University and College accept ultimate responsibility for ensuring that information security is properly managed and that the requirements of this Schedule are implemented and adhered to by the University/College and the University/College Personnel.
2	**Audit**	In addition to any other audit obligations or rights under this Agreement, the University/College will carry out periodic audits to ensure that it is, and the University/College Personnel are, compliant with the requirements of this Schedule and, if required by the Information Commissioner, a senior officer of the University/College will certify

		compliance in writing.
3	**Personnel**	The University/College will ensure that it only uses personnel who have adequate skills, experience and training in the handling of personal data to perform obligations, or exercise rights, which may involve access to the Personal Data. The University/College will ensure that the Personnel are subject to a duty of confidence in respect of the Personal Data.
4		The University/College will maintain a record of all University/College Personnel and the dates on which they are engaged in the Processing of Personal Data.
5	**Staff awareness and training**	The University/College will ensure that all University/College Personnel are aware of their responsibilities when handling and destroying Personal Data and the consequences of non-compliance. In the event of an incident of non-compliance, the University/College will take necessary remedial steps to minimise the risk of repetition, including reminding all persons that process the Personal Data of their responsibilities.
6	**Discipline**	The University/College will reinforce the requirements in this Schedule by disciplinary measures against employees and escalation measures against subcontractors.
GENERAL ORGANISATIONAL MEASURES		
7	**Access**	The University/College will Process the Personal Data and provide access to it on a strictly 'need to know' basis.
8		The University/College will use reasonable endeavours to ensure that Personal Data is kept out of view of any persons who are not involved in performing the Services and will ensure that the Personal Data are not used in any demonstration of the University's/College's capabilities to any other person without data subjects' prior written consent.
9	**Third parties**	The University/College will minimise the authorised disclosure of Personal Data to third parties to the extent reasonably necessary to provide the Services and will, in any event, obtain the prior written consent of their Data

		Protection Officer before making any disclosure.
10	**Security issues**	The University/College will inform their Data Protection Officer(s) immediately if any member of the University's/College's Personnel becomes aware or suspects that: (a)Personal Data have been disclosed or are likely to be disclosed to an unauthorised person; or (b) the University's/College's systems become unavailable or are otherwise compromised so that they cannot function in a manner allowing processing of personal data. The University/College will promptly investigate the cause of the actual or potential disclosure, and take measures to prevent the disclosure where practicable, and/or to prevent any further disclosure.
11		In the event of unauthorised or unlawful disclosure of Personal Data, the University will investigate and co-operate with any enquiries made by the police or the Information Commissioner, and any other regulatory or law enforcement bodies as directed by the Data Protection Officer.
12	**Policies and procedures**	The University/College will ensure that all University/College Personnel comply with the University's data policies (where relevant) and ensure that the Personal Data is protected at least as well as personal data that is or would be under the control of the University/College.
PREMISES and FACILITY SECURITY		
13	**External**	The University/College will provide a physical security perimeter consisting of controlled access, and video surveillance at the premises where the Personal Data are Processed.
14	**Entry controls**	The University/College will ensure that the office areas where Personal Data may be Processed have physical entry controls.
15		The University/College will ensure that all visitor entry and exit is documented at the building reception with date, time of entry, name, purpose or person visited.

16	**Use of Removable Media with Personal Data**	The University/College will ensure that University/College Personnel shall not copy, transmit or transfer Personal Data onto any external hard-drive, laptop, handheld device, removable media, or any personal email account.
17	**Emergencies**	The University/College will ensure that all incidents, including emergencies, that could have compromised the Personal Data are recorded and reported to the Data Protection Officer (s) promptly and, in any event, within 48 hours.
18	**Working away from principal office premises**	The University/College will ensure that University/College Personnel do not process Personal Data outside of the premises of the University.
19		The University/College will ensure that no Personal Data or any device containing Personal Data is left unattended in public view when travelling or in parked vehicles.
20	**Loss or theft**	In the event that a laptop, other handheld device, removable media, print media that contains or is likely to contain Personal Data is lost or stolen, the University/College will ensure that this is reported to the Data Protection Officer(s) without delay and, in any event, within **[**48 hours**]**.
COMPUTER USE		
21	**Environmental controls**	The University/College will ensure that all equipment used in the Processing of Personal Data is protected from physical and environmental threats.
22	**Back ups**	The University/College will ensure that it takes regular back-ups (at least daily) and that all back-ups taken are tracked and are traceable.
23	**Disaster recovery**	The University/College will ensure that it has a disaster recovery plan and that the plan is tested and found to work effectively at least every 6 months.
24	**Access controls**	The University/College will ensure that all computer workstations (desktop, laptop or other) and handheld devices have access controls to prevent unauthorised persons using them.
25		The University/College will ensure that all users have a

		unique, non-obvious password (comprising both numbers and letters) which is required to be changed regularly, as well as in the event of a security breach or the user leaving the employment or service of the University/College.
26		The University/College will ensure that passwords are not written or displayed in any logon dialogue or in any place that readily affords an opportunity for unauthorised individuals to gain access to Personal Data.
27	**Firewalls**	To the extent that any University Personnel may use the University network to process personal data, the University will ensure that all access points to such network(s) are protected by an appropriate firewall.
28	**Virus / vulnerability software**	The University/College will ensure that all systems (including all hardware, disks, media, programs and executables) that are used for the Processing of Personal Data have been checked by appropriate and up-to-date vulnerability scanning and virus checking proprietary software prior to use (and the results are clear). The University/College will ensure that all such systems are regularly checked and achieve a clear result to ensure the security of the Personal Data.
29		The University will ensure that all email attachments and files are virus checked
30		The University/College will ensure that it uses anti spyware software on all of the systems that are used for the Processing of Personal Data.
31	**Software licences**	The University/College will ensure that only licensed copies of software that comply with and do not compromise security are used for the Processing of Personal Data.
32	**Patches and updates**	The University/College will ensure that the latest patches and security updates for software used are applied to its systems and are tested before use on live data.
33	**Downloads and insecure information**	The University/College will ensure that University/College Personnel do not download any software, games, screensavers or other utilities that are not authorised into the University network.

PRINT MEDIA and ELECTRONIC DATA HANDLING		
34	**Transportation of hard copies**	The University/College will ensure that when any paper documents (or other hard media) containing Personal Data are transported or stored they are secured with locks or equivalent devices to prevent tampering and/or unauthorised access.
35	**Copies**	The University/College will ensure that University/College Personnel only copy, reproduce or distribute the Personal Data to the extent necessary to enable the University/College to fulfil its rights and obligations and for no other purpose.
35	**Printing, copying and faxing**	The University/College will ensure that Personal Data are not left unattended at printers, copiers, scanners or fax machines.
37	**Policies and procedures**	The University/College shall adopt a clear desk policy that requires no Personal Data be left unattended and shall ensure that all University/College Personnel comply with it.
38		The University/College shall ensure that all University/College Personnel use screen savers and/or lock their computer screen when away from desks.
39	**Encryption**	The University/College will ensure that all Personal Data (stored in any form and media whether tangible or intangible) that include sensitive personal data, or which would cause damage or distress to a data subject if lost, stolen or accessed by an unauthorised person, are encrypted, especially when in transit between systems or held on mobile devices or exchangeable media.
40	**Emails**	The University/College will ensure that University/College Personnel do not use the 'Reply to All' feature in emails which contain, or have an attachment containing, Personal Data.
41		The University/College will ensure that University/College Personnel do not use group email addresses when emailing any Personal Data unless all members of the group are authorised to receive the Personal Data.
42		The University/College will ensure that University/College

		Personnel do not use the blind copy feature in emails which contain, or have an attachment containing, Personal Data.
43		The University/College will ensure that emails that are suspicious or of unknown origin are not opened where this could compromise the Personal Data.
44		The University will ensure that its email systems use spam filters.
FAXES		
45	**Alternatives**	The University/College will ensure that faxes including any Personal Data are only sent when no other communication method is appropriate such as secure email, telephone conversation or a secure courier service.
46	**Fax numbers**	The University/College will ensure that University/College Personnel check fax numbers are correct before sending a fax that includes any Personal Data.
47	**Recipients**	The University/College will ensure that faxes that include any Personal Data are only sent to recipients that are expecting to receive the fax and have appropriate measures in place to ensure the security of the Personal Data on receipt.
48	**Receipt**	The University/College shall ensure that any fax sent that includes any Personal Data has been received by obtaining confirmation from the intended recipient.
49	**Cover sheets**	The University/College will ensure that University/College Personnel use a cover sheet for each fax sent that includes any Personal Data which states the number of pages being transmitted, the name of the intended recipient, the fact that the content is confidential and not to be read by anyone other than the named intended recipient and who to contact with a telephone number in the event of a transmission error or other issue that could compromise the Personal Data.
DESTRUCTION		
50	**Print media**	The University/College will ensure that all print media that contains Personal Data is securely destroyed (e.g. by

incineration or shredding) as soon as reasonably possible (and must be kept secure in a locked cabinet or locked waste bin in the interim).

51 The University/College will ensure that misprinted copies that contain Personal Data are stored securely until destruction and are securely destroyed (e.g. by incineration or shredding) as soon as reasonably possible.

52 **Hardware** The University/College will securely destroy all Personal Data held on hardware and exchangeable media before disposing of an old device by using appropriate technology or destroying the hard disk.