Improving Working Memory

National Institute of Economic and Social Research and Behavioural Insights Team

Education Endowment Foundation

Evaluation Summary	
Age range	Year 3 (age 7-8)
Number of pupils	Around 1,700
Number of schools	115
Design	Cluster randomised trial
Primary Outcome	Number skills, assessed using British Ability Scales, 3rd Edition

Intervention

The intervention is delivered to year 3 pupils, and is designed to try to help pupils who are behind the class average in numeracy. It is expected that a substantial proportion of these children might have lower performance in working memory. The intervention combines two aspects of working memory training: strategies and practice. The strategies (rehearsal, association, using fingers) are taught by Teaching Assistants (TAs) in structured sessions, with support from computer games. Practice is encouraged by use of the computer games. The TAs will be trained by Oxford (the project team) in a one-day training, along with a link teacher at each school. Oxford and the link teacher monitor and support implementation. The tuition and computer game time take place additionally to maths teaching.

A modified version of the intervention that is blended with games from the mathematical reasoning curriculum will also be tested in this trial (if a sufficient number of schools can be recruited – see below). The rationale is that pupils who are behind in their maths may require additional help with working memory, but also with maths-specific content. This blended intervention will be delivered over the same time period.

The trial will therefore potentially have three arms. The Working Memory (WM) intervention and the blended working memory and number skills (WM+) intervention will be compared with a control group. The WM and WM+ interventions will be of the same length. Some variation in the expected length of delivery is likely in practice. Schools will be directed to allocate a total of 8-10 hours TA time (with a 50/50 split between TA time and games) over the course of a term.

Significance

Working memory is the ability to remember and manipulate information over short time-frames. Training memory as a means of increasing attainment has foundations in cognitive science (Baddeley, 2000). Working memory has been shown to be a reliable predictor of attainment in numeracy (Baddeley et al., 2011). Consequently, being able to improve working memory appears to offer a means of raising attainment among lower-performing children.

The Working Memory programme developed by the team at Oxford University (Nunes et al., 2008, 2011, 2014) has been tested in two control group studies, one with hearing children and one with deaf children. These two studies involved small numbers of children, 35 and 153 respectively.

However, they do provide promising results with both suggesting that the intervention positively impacts on working memory, with effect sizes of between 0.26 - 1.2 standard deviations.

Therefore the intervention is ready for an efficacy trial with attainment and working memory tested as outcomes.

Research questions

The primary research question this evaluation is designed to answer is:

- What is the effect of WM and WM+ on children's number skills at the end of year 3?

The evaluation will also estimate the impact of WM and WM+ on the following secondary outcomes:

- Working memory at the end of year 3
- Attention and behaviour in class at the end of year 3.

Impact will also be estimated separately for pupils receiving free schools meals.

Design

This will be a cluster randomised trial. Randomisation will be at school level. The number of arms depends on how many schools are recruited. The target is to recruit 115 schools and to have three arms – WM, WM+ and control. If the number of schools recruited falls below 110, the trial will have only two arms (WM and control). The control group will be a 'business as usual' control where schools are expected to continue with normal classroom teaching and support for eligible pupils.

Randomisation

Blocking will be used to improve cross-arm comparability of schools and also to improve precision of estimates. There will be six blocks, defined on the basis of school size (one-form entry, two or more form entry) and most recent school KS1 performance (lower third, middle third, upper third).

Randomisation will be designed to achieve an equal number of schools in each arm:

- Each school will be assigned a randomly generated number
- Schools will be sorted by block and random number
- In the two arm case
    - Schools will be assigned to the WM arm then the control arm in turn
- In the three arm case
    - Schools will be assigned to the WM arm, then the WM+ arm then the control arm in turn

The computer code used to carry out the randomisation will be recorded and reported in the final report.

Participants

English state primary schools will be eligible to participate in the trial, provided they have at least 20 pupils in Year 3. Schools will be recruited by Oxford. Schools will be directly approached through letters inviting them to participate and indirectly approached through the Yorkshire advocates. Invitations will also be available in the website of the Department of Education, University of Oxford, and the website of the Oxford University Press. Fliers about the project will be distributed at

different events in which members of the team will have the opportunity to meet school representatives (e.g. teachers, numeracy experts).

Schools will be required to identify eligible pupils from Year 3 prior to randomisation. They will be asked to select a minimum of 10 and maximum of 20 (if 2 form entry or more) pupils. Teachers will be asked to select those pupils they view as having the lowest number skills in the year group.

Schools wishing to participate in the trial will be asked to sign a Memorandum of Understanding, and must be willing to fully comply with the requirements of the trial, including supplying the necessary pupil data. Opt-out consent will be sought from parents of all eligible pupils for agreement for data sharing. Schools in the control group will be given a financial incentive that they can then spend on the training, if they wish, after the post-test.

Outcome Measures

The primary outcome is:

- Number skills. This will be assessed at the end of year 3 using the BAS3 number skills test. The tests will be administered by research assistants recruited by BIT, blinded to allocation status. There is no pre-test but instead KS1 scores will be used.

The evaluation will consider two secondary outcomes:

- Working memory. This will be assessed prior to randomisation before the intervention and also at the end of year 3 using the three central executive subtests (counting recall, backward digit recall, listening recall) of a working memory scale for children (Pickering & Gathercole, 2001, or Alloway, 2007, which is the computerised version). It will be administered by Oxford's researchers, blinded to allocation status. This will involve RAs from BIT auditing a random sample of the assessments to ensure that they are completed as per the protocol and that assessors are blind to the allocation of the child.
- Attention and behaviour in class, as assessed by teachers at the end of year 3. When testers visit schools for data collection on the WM test, they will approach teachers, who will be asked to complete 15 items for the "Attention Rating Scale for Teachers" (adapted from the original by James M. Swanson; Swanson et al., 2001). This is a 4-point rating scale which contains items relevant to children's sustained attention in the classroom. There is no specific training required of raters, beyond the instructions. The Oxford team will be responsible for data entry. Data will be shared with the evaluation team, once available.

Only those eligible for the intervention will be tested (treatment and control arms).

Sample size calculations

We will have 115 schools with 10-20 pupils per school; the power calculations are based on a simplifying assumption of 16 per school. Further assuming 88% are observed in the data (this is informed by Worth et al., 2015), this will result in about 14 useable pupils per school, on average. In light of the Worth et al., (2015) results, we assume an intra-cluster correlation of 0.12. We will have two pre-tests; KS1 results and Working Memory baseline assessment. The Worth et al., (2015) results suggest covariates accounted for 57% of the variance at both school and individual levels. The same is assumed in calculating the minimum detectable effect size (MDES) for this trial. The MDES is calculated on the basis of a 2-tailed, with 95% significance and 80% power.

Under these assumptions, a 3-arm trial has a MDES of 0.18. Should the number of schools recruited fall below 110, the trial will have only two arms. With two arms, power is increased. For example, a 2-arm trial with 110 schools gives a MDES of 0.15. The MDES achieved with a 3-arm trial of 115 schools is achieved in the 2-arm case with 76 schools.

The trial will also produce impacts for the FSM subgroup. Assuming 15% of children are FSM, this reduces the average assumed cluster size to roughly 2, although since there is likely to be a correlation between FSM and pupil level eligibility this is perhaps conservative, with the cluster size somewhat higher. However, with 2 per cluster, the FSM subgroup MDES corresponding to the two 3- and 2-arm cases described above are 0.32 and 0.26.

Analysis plan

See Appendix 1.

Implementation and process evaluation methods

The objective of a process evaluation is to establish fidelity and identify the factors which might influence and explain impact. We would also look for evidence of effectiveness which cannot be obtained statistically and issues which would need to be considered for a wider roll out of the intervention. This might include how pupils respond to each of the programmes and aspects of the TA/pupil relationship. The process study will be informed by a theory of change that will be developed early in the project and registered as an update to the protocol.

The basic features of our design are:

- Attendance at and evaluation of TA training
- Analysis of project materials and of qualitative data collected by the project team during visits to schools.
- Visits to 8 schools (4 from each treatment arm) to interview TAs, link teachers and senior leaders and observe sessions
- On-line surveys of all intervention and control schools, with questions on implementation for project leads
- Analysis of quantitative data on fidelity and dosage and how it moderates treatment effect (e.g. number of games and units completed or length of time spent with TA)

Evaluation of training: We will attend training courses held for link teachers and TAs to understand their initial experiences of the intervention, their expectations and any concerns. We will also review training content and materials to understand how link teachers and TAs are prepared to deliver the intervention. We will also review monitoring and support provided by the project teams to schools and TAs.

Review of materials: We will review materials developed by Oxford University and used by TAs. This will also be covered in interviews with TAs and in observation of sessions (see below). We will also review online games selected to be used within the trial. Members of the project team at Oxford will collect the children's record sheet at the end of the programme. We will use extracted data from the record sheets. More generally, we would expect to work closely with the Oxford team to share qualitative and quantitative data collected during the course of the intervention relevant to the process evaluation.

Case studies of selected schools will be carried out to examine the implementation of IWM in depth. Through visits to 8 schools, we will carry out interviews with link teachers, TAs and senior leaders. If the trial is 3 armed, case study schools will consist of 4 WM and WM+. Schools will be selected to include a range by factors such as pupil characteristics and school performance. Topics covered in the interviews will include views on the training, materials and approach, including fidelity to the planned intervention. Interviews with senior leaders would explore contextual issues, including school performance for maths and identified barriers to improvement. It would also establish other strategies in place to improve maths performance. We will also observe a sample of improving working memory sessions. Interviews will be digitally recorded, with the agreement of research participants, and transcribed. TA support sessions with pupils will be observed, using a pro-forma which we will design for the purpose. It will focus on the appeal of IWM and will include qualitative assessment of pupil engagement. Data will be analysed using a social research 'framework' approach, drawing themes and messages from an analysis of interview transcripts and other materials collected by evaluation and project teams. NIESR will consult with the EEF and Oxford on timings but would expect case study visits to take place towards the end of treatment delivery.

Online survey of all schools: Our fieldwork will only be with a sample of schools. It will be important to gather qualitative data in a consistent way from all schools on implementation and perceived outcomes and on factors which could affect fidelity. This will include what classes children miss through attending WM or WM+ sessions, previous or on-going work on improving memory and on maths improvement work and particularly any approaches which are centred on memory. Project leads in the intervention schools will be surveyed at the end of the term in which the project is delivered. Following an email to link teachers in advance from the Oxford team, NIESR will email these individuals again with a link to a short on-line survey. Non-responding schools will be sent two reminders. Control group schools will also be surveyed, about their existing approaches of relevance to the intervention, which might potentially affect measurable impact of the intervention in test schools. As with the intervention schools, the project team will provide an email introduction, after which NIESR will send a link to an on-line survey, along with two reminders.

Costs

The process evaluation will include consideration of resource implications and hidden costs. During the visits to schools we would also discuss the costs of the project to schools. The purpose of collecting such data in the process evaluation would be to identify areas of expenditure that the project entails and which would need to be considered for a wider roll out of the project. These might include additional equipment or time to liaise with parents. We can also include a question on additional costs in the survey of all WM and WM+ schools.

Ethics and registration

Ethical review of the project is being undertaken by the University of Oxford.

Parents will be provided with an information sheet giving details of the aims of the research. This form will offer parents (or legal guardians) the opportunity to opt out of the trial. It will also offer the opportunity for parents to withhold consent to accessing their child(ren)'s National Pupil Database records. We judge opt-out consent is sufficient for NPD data linkage in this case

Data will be transmitted and stored using the security principles underlined in the institutional Data Security policies (attached in Appendices 2, 3 and 4) and the procedures set out in further detail for

this specific project in the Data Sharing Agreement (attached in Appendix 5). This includes secure transfer of data and use of password-protection and encryption as appropriate during data storage.

The trial will be registered at www.controlled-trials.com.

Personnel

Project team

Terezinha Nunes, Peter Bryant, Rossana Barros Baertl, Deborah Evans, Susan Baker – Oxford University

Evaluation team

Richard Dorsett (Principal Investigator), Jake Anders, Nathan Hudson-Sharp, Heather Rolfe – NIESR.
Aisling Ní Chonaire, Michael Sanders, Francesca Tamma - BIT

The teams will have the following roles within the evaluation:

Design of the trial

- sample size calculations - NIESR
- refinement of randomisation approach - NIESR

Delivery of the intervention

- recruitment of schools - Oxford
- delivery of training – Oxford

Measurement of outcomes

- number skills – BIT
- working memory – Oxford
- attention and behaviour – Oxford
- application and linkage to KS1 outcomes – NIESR

Impact analysis – NIESR and BIT
Qualitative analysis - NIESR

Risks

The data security policies of BIT, NIESR and Oxford and the Data Sharing Agreement between BIT, NIESR and Oxford are included with this protocol.

Some of the key risks are listed below:

- School drop-out after randomisation reduces the integrity of the experimental design. To reduce the risk of drop-out, it will be important to ensure schools are well-informed about the programme and the trial from the start, so that they are clear as to what is expected of them before they commit to taking part. Schools will be asked to sign a memorandum of understanding as a signal of their commitment. It will also be important to maintain good communications with schools throughout the project in order to maximise retention. It is also very important for the teams to have good communications and for the evaluation team

to send their communications to schools to Oxford before they are sent to schools. Drop-out of control schools is a particular risk; to help minimise this control schools will be offered the option to receive programme at later date.

- There may also be difficulties in recruiting schools to the trial. Records will be kept of schools approached and where possible, their reasons for not participating, to provide an indication of external validity.
- If individuals do not consent to data sharing this has the potential to reduce the sample size, and affect the internal and external validity of the trial. As consent is collected pre-randomisation, it should not affect the internal validity of the trial, as any withholding of consent should be just as prevalent in the treatment and control groups. In addition, as only opt-out consent is required, we judge that the risk of a large number of opt-outs is low.
- If pupils are not present on the day of testing this may also reduce the sample size by reducing the number of pupils for whom we are able to obtain a post-test; furthermore, it may introduce some bias if it is a non-random group of pupils who are absent. When arranging dates for tests, the question of how times can be chosen to minimise absenteeism will be discussed with the schools. In those where a higher proportion of pupils are absent, mop-up visits will be carried out to attempt to minimise this risk.
- There is a possibility that the delivery of the intervention will vary across schools. However, this reflects the reality of implementing such a programme; impact estimates therefore relate more to type of treatment likely to prevail in practice rather than that which might be observed under ideal conditions. Nevertheless understanding treatment variation is important and will be explored as part of the process evaluation.
- When randomising clusters rather than individuals the chances of a 'bad draw' increase because of the smaller number of units. We will use blocking to limit the likelihood of this.

Timeline

Date	Activity
Jan 2016 - August 2016	Development of WM+ intervention and recruitment of schools (Oxford) - obtain ethical approval
Sept - October 2016	Identification of pupils by teachers - Administer working memory pre-test (Oxford)
	Randomisation (NIESR). To be carried out after pre-test
Nov - Dec 2016	Training of TAs (Oxford)
Dec 2016	Linkage to KS1 pre-test (NIESR)
Jan - May 2017	Delivery of programme (Oxford)
Oct 2016 - May 2017	Process evaluation ongoing throughout this period (NIESR)
May-Jun - 2017	Administer numeracy post-tests (BIT)
	Administer working memory and attention and memory post-test (Oxford)
Aug - Sep 2017	Impact analysis ongoing throughout this period (NIESR, BIT)
Dec 2017	Evaluation report (NIESR, BIT)

References

Baddeley A. (2000) The episodic buffer: a new component of working memory? Trends Cogn Sci 4: 417-23.

Baddeley A., Allen R., Hitch G. (2011) Binding in visual workingmemory: the role of the episodic buffer. Neuropsychologia 49: 1393-400.

Nunes, T., Evans, D., Bell, D. & Campos, T. (2008) Improving children's working memory through guided rehearsal. Paper presented at the AERA meeting, 2008, New York.

Nunes, T., Barros, R., Evans, E., Burman, D. (2011) A game-based working memory intervention for deaf children. Serious Games, 280: 31-39.

Nunes, T., Barros, R., Evans, D., & Burman, D. (2014). Improving Deaf Children's Working Memory through Training. International Journal of Speech & Language Pathology and Audiology, 2, 51-66. E-ISSN: 2311-1917/14.

Swanson JM, Kraemer HC, Hinshaw SP, Arnold LE, Conners CK, Abikoff HB, et al. Clinical relevance of the primary findings of the MTA: success rates based on severity of ADHD and ODD symptoms at the end of treatment. J Am Acad Child Adolesc Psychiatry. 2001;40(2):168-79.

Worth, J., Sizmur, J., Ager, R. & Styles, B. (2015) "Improving numeracy and literacy" EEF evaluation report.

Appendix 1: Analysis Plan

Trial objective

To estimate the impact of training working memory on:

- number skills.

In addition, the trial will estimate the impact of training working memory on two secondary outcomes:

- working memory
- attention and behaviour in class.

Sample size

We have a target of 115 schools with 10-20 pupils per school; our power calculations are based on a simplifying assumption of 16 per school. Based on the results of a previous trial,[1] we further assume:

- 88% are observed in the data (implying about 14 useable pupils per school, on average)
- an intra-cluster correlation of 0.12
- covariates accounted for 57% of the variance at both school and individual levels.

The minimum detectable effect size (MDES) is calculated on the basis of a 2-tailed, with 95% significance and 80% power.

Under these assumptions, a 3-arm trial has a MDES of 0.18. Should the number of schools recruited fall below 110, the trial will have only two arms. With two arms, power is increased. For example, a 2-arm trial with 110 schools gives a MDES of 0.15. The MDES achieved with a 3-arm trial of 115 schools is achieved in the 2-arm case with 76 schools.

Randomisation

Schools will be categorised on the basis of school size (one-form entry, two or more form entry) and most recent school KS1 performance (lower third, middle third, upper third). This will result in six blocks. Within each block, schools will have their treatment condition randomised. The purpose of this blocking is to improve cross-arm comparability of schools and also to increase precision of estimates.

Randomisation will be implement in a way that achieves an equal number of schools in each arm:

- Each school will be assigned a randomly generated number

[1] Worth, J., Sizmur, J., Ager, R. & Styles, B. (2015) "Improving numeracy and literacy" EEF evaluation report.

- Schools will be sorted by block and random number
    - In the two arm case, schools will be assigned to the WM arm then the control arm in turn
    - In the three arm case, schools will be assigned to the WM arm, then the WM+ arm then the control arm in turn

The computer code used to carry out the randomisation will be recorded and reported in the final report.

Outcomes

The primary outcome is:

Number skills. This will be assessed at the end of year 3 using the BAS3 number skills test. There is no pre-test but instead KS1 scores will be used.

The evaluation will consider two secondary outcomes:

Working memory. This will be assessed prior to randomisation before the intervention and also at the end of year 3 using the three central executive subtests (counting recall, backward digit recall, listening recall) of a working memory scale for children. The pre-randomisation measure will be used as a pre-test.

Attention and behaviour in class, as assessed by teachers at the end of year 3, who will be asked to complete 15 items for the "Attention Rating Scale for Teachers". There is no pre-test but instead KS1 scores will be used.

Analysis

Analysis will be conducted on an intention-to-treat basis, including all children matched to groups. Analyses will be conducted in STATA version 13, using 2-sided significance tests, at 5% significance level.

Baseline characteristics

Baseline characteristics observed in the National Pupil Database (gender, age, Key Stage 1 maths scores, ethnicity, EAL, SEN, FSM, attendance, IMD) will be summarised by treatment arm.

Trial completion

CONSORT diagram will be used to present summary of the flow of eligible children and their schools from recruitment through randomisation, post intervention assessment and analysis. The number of children and schools included or excluded at each stage will be clearly stated and the reasons for exclusion will also be stated.

Primary analysis

The primary analysis will compare the outcomes of those with a Working Memory treatment against a `business as usual' control group. In the case of a three-arm trial, two variants of Working Memory training will be trialled; children in the the 'WM' group of schools will

receive the Working Memory training on its own, children in the the 'WM+' group of schools will have the WM training complemented with number skills training. In the case of a two-arm trial, there will be only the WM group and the control group.

The impacts of the intervention will be estimated using linear regression models. Outcome variables will be regressed on treatment arm indicators, block indicators, and KS1. Inference will be based on standard errors adjusted for school-level clustering using Stata's 'cluster' option. This is reasonable in view of the large number of schools involved. We will report the distribution of missing observations by treatment arm and explore whether baseline characteristics are balanced across arms for the complete-case sample.

The estimated impacts will be "intention to treat" (ITT) effects and will be reported with 95% confidence intervals. Effect sizes will be calculated using the Hedges' g formula. This will require estimates of the standard deviation for the treatment and control groups, which can be derived from the estimated regression. Intra-cluster correlations will be reported.

We will also conduct the analysis for the subgroup of pupils who have ever received free schools meals using the variable FSMever from the National Pupil Database.

Appendix 2: University of Oxford Department of Education Information Security Policy

Separate document attached.

Department of Education

Information Security Policy

1. Context, Purpose & Scope

1.1. The Department of Education (the Department) handles a wide range of information and this information is essential to its teaching, research and administrative activities. The Department recognises the need for its staff, students and visitors to have access to the information they require in order to carry out their work and recognises the role of Information Security in enabling this.

1.2. This policy is designed to ensure that the Department complies with all relevant University and legal requirements in respect of Information Security.

1.3. The purpose of this Information Security Policy is to protect the security of the Department's information assets from all threats, whether internal or external, deliberate or accidental. Information will be protected from loss of: confidentiality, integrity and availability.

1.4. This policy is intended for all staff, students, visitors and collaborators using the Department's IT systems, data or any other information asset.

2. Roles and Responsibilities

2.1. This policy is approved by the Departmental Board.

2.2. The Department's Director is ultimately responsible for the maintenance and implementation of this policy within the Department.

2.3. The Head of Administration & Finance will act as the Information Security Co-ordinator, with support from the Department's IT Manager.

2.4. The Resources & IT Committee is responsible for both identifying and assessing security requirements and risks and recommending mitigating actions to the Departmental Board. It is also responsible for reviewing this policy on an annual basis and making recommendations on any changes required to the Departmental Board.

2.5. Line Managers, supervisors and sponsors are responsible for ensuring that all staff and visitors for whom they are responsible are made aware of this policy and given appropriate support and resources in order that they may comply with it.

2.6. Where staff have any questions or concerns about information security they should contact their line-manager, supervisor or sponsor in the first instance, or the Information Security Co-ordinator and/or IT Manager.

2.7. It is the responsibility of each person using the Department's IT systems, data or any other information asset to comply with this policy.

3. Incident Reporting

3.1. Any suspected breach of the Information Security Policy outlined in this document must be reported to the Information Security Co-ordinator promptly.

3.2. In the event of a reported suspected breach the Information Security Co-ordinator will ensure that the Department adheres to the University incident response procedures.

4. General Procedures and Practices

4.1. Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data e.g. lock away hard copy confidential documents, do not read confidential information in a public place, do not leave confidential information on a photocopier or printer.

4.2. Where possible confidential data should be stored on departmental file servers and not on local hard drives unless approved encryption is used to secure the data.

4.3. Confidential information should be downloaded from secure University systems (e.g. Oracle Financials, HRIS) only when strictly necessary for the purposes of your role.

4.4. Passwords must not be shared or disclosed to any third party.

4.5. Staff, students and visitors must obtain explicit authorisation from their line managers (or equivalent) for the storage, exchange or synching of confidential data using either free or commercial cloud storage services (e.g. Dropbox, SkyDrive, Google Docs etc.).

5. Email

5.1. Email should not be considered totally secure. If you are thinking of sending confidential information via email please carefully assess the risks, e.g. how sensitive is the information? What are the risks of the email not reaching the right person? Is the content such that other parties would wish to "hack" the email?

5.2. If the risks are high and you are sharing data within the University consider using an alternative to email such as WebLearn or SharePoint to share confidential data.

5.3. If the risks are high and you are sharing data outside of the University you should encrypt the confidential data held within the email. Further detail is available from the IT Manager.

5.4. Take care to ensure that emails containing confidential data are sent to the correct address. Do not rely solely on any "autocomplete" function for the email address and take care when selecting an address from any directory, address book or contacts list.

5.5. If you receive confidential information inadvertently via email, you should delete it as soon as possible.

5.6. Please ensure you take general precautions to safeguard your email account such as using strong passwords, not responding to phishing or spam emails and by not giving your password to anyone else.

6. Mobile Devices (Laptops, Phones, Tablets) & Removable Media (USB drives)

6.1. Mobile devices used to handle confidential information must be appropriately secured. A password must be applied to all such devices and they must be kept updated with the latest security patches to their software. Many devices allow you to set an 8 digit password and this should be enabled if possible.

6.2. This policy applies to all mobile devices whether they are owned by the Department or personally-owned i.e. if a device is used for any work-related purpose and the data is considered confidential.

6.3. Confidential data must be encrypted, using AES 256bit encryption or stronger, when stored on mobiles devices or removable media.

6.4. Further detail is available from the IT Manager

7. Off-Site & Remote Access

7.1. Only trusted machines, not public kiosk machines (e.g. airports, hotels and coffee shops), should be used to connect to the University network remotely.

7.2. Home computers used to access University systems must be kept secure through firewalls, anti-virus software and security updates.

7.3. Whenever possible all connections to University systems should be made over the Virtual Private Network (VPN) as an additional security measure.

8. Information Handling & Disposal

8.1. All confidential data must be stored securely; in a locked cupboard or office or, if stored electronically, then secured using appropriate access permissions agreed with the data owner.

8.2. All confidential data must be removed from office equipment (e.g. filing cabinets, desks) prior to re-use or disposal.

8.3. Confidential documents must be shredded when no longer needed (locked bins for paper to be removed for secure shredding are provided within the Department).

8.4. Surplus or obsolete computers, mobiles devices and removable media must be sent to the Department's IT Team for data cleansing and recycling or destruction.

9. Building Security

9.1. All external doors to the Department's buildings will be locked at all times, as regulated access to buildings is the first line of security. Internal offices must be locked when not in use, unless these are emergency exits.

9.2. Members of the Department will be issued with swipe cards and keys that are appropriate to their level of work. If a member of the Department loses their swipe card or keys they must notify the administration team immediately. Members of the Department must not give their room keys or swipe cards to any third party.

Annexe A: Definition of Confidential Information

Confidential information is any information that is not intended to be publicly available. If the loss or unauthorised disclosure of information could have adverse consequences for the University or individuals, it is confidential.

Given the potentially serious consequences of breaching the Data Protection Act (DPA), you should assume that all personal data is confidential. Personal data is any data that identifies a living individual e.g. a CV, email address, reference, job or course application, home contact details, etc.

The following list consists of generic examples and is for the purpose of illustration only.

Examples of Personal data[1]

1. Any set of data that could be used for fraud or identity theft, including but not limited to bank account or credit card details, national insurance number, passport number, home address, date of birth.

2. Data relating to an individual's application for a job, performance in a job interview, work performance, promotion or disciplinary record

3. Data relating to a student's academic performance or disciplinary record

4. Data relating to an individual's personal or family life e.g. their interests, hobbies, relationships

5. Any sensitive personal data, as defined in the DPA i.e. information relating to:
    - health (mental or physical),including disabilities and genetic predispositions
    - ethnicity or race
    - sexual life
    - trade union membership
    - political opinions
    - religious beliefs
    - commission or alleged commission of a criminal offences
    - criminal proceedings

Examples of Business information

1. Information provided to the University on the understanding that it is confidential, whether explicit or assumed

2. Information the disclosure of which would disadvantage the University's position in negotiations, whether commercial or otherwise

3. Reorganisation or restructuring proposals that would have a significant impact on individuals, prior to a decision being announced

4. Exam questions before the examination takes place

5. Security arrangements for buildings or for high profile visitors or events

6. Papers discussing proposed changes to policies or procedures on high profile or sensitive issues, before the changes are announced

[1] Any recorded information, hard copy or electronic, which identifies a living individual e.g. name, e-mail address, reference, CV, photograph.

Annexe B: Relevant Legislation, University Policies, Regulations & Sources

Legislation:

i. Data Protection Act (1988): http://www.legislation.gov.uk/ukpga/1998/29/contents

University Policies and Regulations

ii. University Regulations Relating to the use of Information Technology Facilities: http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml
iii. University Information Security Policy: http://www.it.ox.ac.uk/infosec/ispolicy/
iv. JANET(UK) Statement of acceptable use Policy: https://community.ja.net/library/acceptable-use-policy
v. University Policy on Data Protection: http://www.admin.ox.ac.uk/dataprotection/
vi. University Policy on Freedom of Information: http://www.admin.ox.ac.uk/foi/
vii. University Privacy Policy: http://www.admin.ox.ac.uk/dataprotection/privacypolicy/
viii. Trade Mark and Domain Name Policy: http://www.admin.ox.ac.uk/lso/faq/#d.en.30994
ix. Mobile Wireless Networking Regulations: http://www.oucs.ox.ac.uk/network/wireless/rules/index.xml?splitLevel=-1
x. Rules for University Web Sites: http://www.ox.ac.uk/web/rules/
xi. Computer disposal: http://www.ict.ox.ac.uk/oxford/disposal/
xii. Handling Illegal Material: http://www.ict.ox.ac.uk/oxford/rules/soaguidelines.xml
xiii. Other related policies can be viewed here: http://www.it.ox.ac.uk/legal/rules/

Sources:

xiv. Example policies and wording from here: http://www.it.ox.ac.uk/infosec/istoolkit/tools/
xv. Data classifications: http://www.it.ox.ac.uk/media/global/wwwitservicesoxacuk/sectionimages/security/classification_scheme26.08.11.pdf & http://www.ictf.ox.ac.uk/conference/2013/presentations/wks-a1-tightening-it-security.pdf (accessible to IT Support Staff only)

Appendix 3: NIESR Data Protection Policy

Separate document attached.

Third Party Data Security Policy

National Institute of Economic and Social Research (NIESR)

Contents

Executive Summary

NIESR receives and uses data provided by 3rd parties to carry out their research.

This data must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998.

NIESR regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals.

The purpose of this policy is to ensure that the staff, volunteers and trustees of NIESR are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

All data that NIESR receives should be classified according to its sensitivity. Data should be stored, accessed and processed according to their classification.

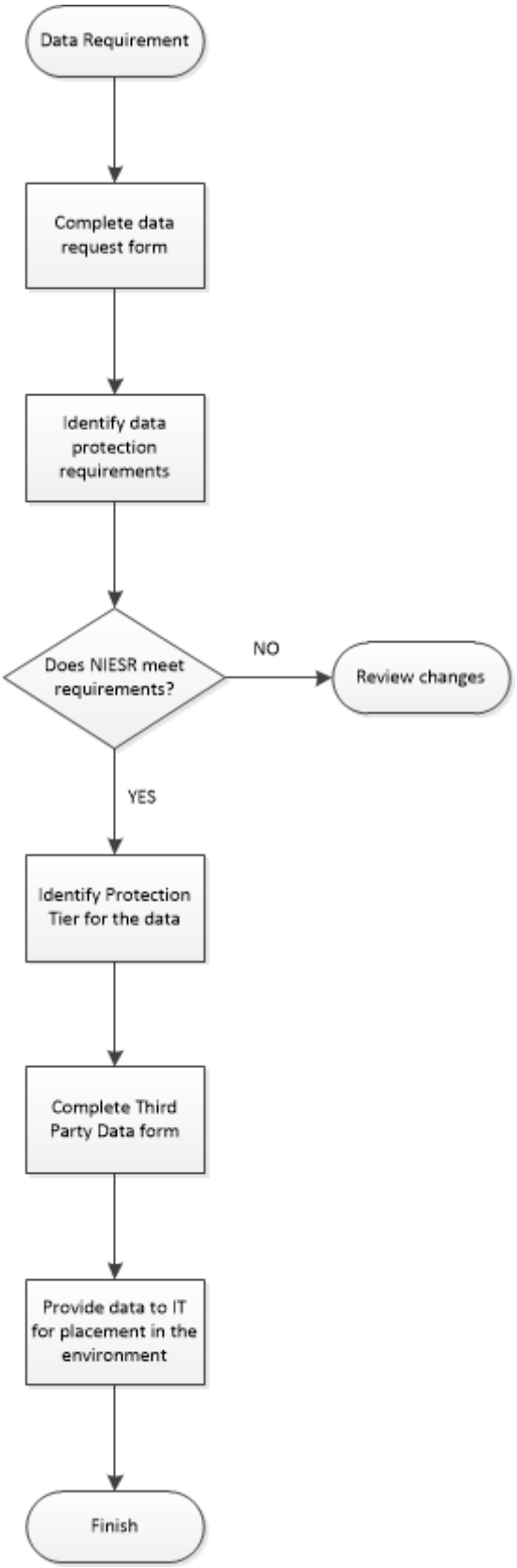
The classification of data is an important component to knowing how to use the data within the guidelines laid down by the data providers.

Correctly classifying data and then using it only according to the appropriate stipulations is an important part of preventing data leaks, and minimising the impact of such leaks when they do occur.

Inappropriate disclosure of Confidential or Restricted data, their accidental loss or deliberate theft, could all lead to the Institute being levied with a potentially unlimited fine, as well as experiencing a loss of reputation and a possible failure to win other research contracts.

Third Party Data Acquisition Process

The generic process for third party data to be acquired by NIESR is shown below



Physical Security

The following section details the physical security in place at NIESR.

External Access

1. External doors into the building are secured and cannot be opened from outside the building.
2. Visitors must identify themselves before entering the building and must sign-in the visitors' book on arrival.
3. Visitors must identify to receptionists a specific individual that they have come to meet with.
4. Visitors are not allowed to leave the reception area unattended.
5. Devices storing the third party data should be in physically secure, restricted areas where only allowed individuals have access.

Infrastructure Servers

6. Servers storing 3rd party data are located in a locked server room.
7. Only specifically allowed individuals have access to the server room.
8. Servers are secured in purpose built racking.

Personal Computers

9. Personal computers storing 3rd party data must be located in locked rooms.
10. Only specific individuals will have access to the rooms.
11. Only prescribed computers may store 3rd party data
12. Computers storing 3rd party data must meet all organisational security requirements for the data tier and these machines will be restricted from ANY usage when not connected via physical or remote secure connection to the NIESR network

Laptop Computers and Mobile Devices

13. 3rd party data must not leave the premises or the NIESR network without authorisation and therefore must not be stored on laptop computers or mobile devices.
14. Data will only be stored on tracked NIESR devices that meet the security requirements

Network Security

The following section details the network security in place at NIESR.

Perimeter Security

15. The NIESR network is protected at the perimeter by a firewall device. The firewall prevents external traffic or connections into the NIESR network unless specifically allowed.
16. The NIESR firewall allows the following:
    - 16.1. Remote VPN connections
    - 16.2. HTTPS connections
    - 16.3. HTTP connections
    - 16.4. Authorised FTP outbound connections
    - 16.5. No inbound FTP connections
    - 16.6. Authorised SFTP connections
    - 16.7. SMTP connections

Authentication

17. NIESR operates a Microsoft Active Directory authentication service. No user logon to a device connected to the network is allowed without a valid Username and Password.
18. Passwords must meet minimum security requirements
19. Passwords will be changed every 30 days
20. Password sharing or use of other user's credentials is prohibited
21. All physical devices will be restricted by MAC address. No devices may be connected to the network without prior approval / authorisation

Permissions

22. All users / devices must be authenticated
23. Alteration to permissions must be authorised in writing by an approval group

Data Security

The following section details the data security in place at NIESR.

Data Storage

24. NIESR categorise data received from 3rd parties. There are three tiers of categorisation:
    - 24.1. Protected – data within this tier is stored in an area that is only accessible to network users that have provided an authenticated Username and Password and are allowed access to network resources.
    - 24.2. Restricted – data within this tier is stored in an area that is only accessible to users that are specifically allowed access to the data.
    - 24.3. Confidential – data within this tier is stored in an area that is only accessible to users that are specifically allowed access to the data; in addition the data is encrypted when stored.
25. When data is received from a 3rd party the data security category is formally agreed with NIESR and the data stored accordingly.

Data Removal

26. When the data is no longer required it must be completely removed using Data Removal Tool to completely delete data from the disk. PGP software is used for data destruction. We have the ability to complete multi pass wipes, PGP Freespace Wipe carries out 26 passes for maximum security. Any hardware we dispose of is done in a WEEE compliant way and we can provide certificates.
27. Any paper copies of 3rd party data that are received or created are destroyed by shredding with a device capable of DIN Level 5 shredding.

Data Backup

28. For the data received from 3rd parties there is often no requirement for backups. If it is necessary for NIESR to backup this data it will be backed up to an internal storage platform. The data will be encrypted in transit and when it is located on the storage.
    - 28.1. All data will be backed up a minimum of 1 copy
    - 28.2. Data will be kept for 6 months at least one copy
    - 28.3. Varying data will keep all variations up to 5 copies
    - 28.4. All data will be stored offsite

28.5. Backups will be encrypted and the encryption key is to be held only by NIESR for confidential data

Portable Media

29. To prevent the movement of data out of the NIESR managed environment and insecure storage of the data portable media will be blocked on personal computers involved with 3rd party data.

Physical Media

30. All physical media containing 3rd party data will be stored in a locked filing cabinet.
31. Physical media will be encrypted
32. Physical media will be asset tagged and it will be checked in/out before and after use

Access Monitoring

33. Access to the data provided by 3rd parties will be monitored to identify individuals accessing.
34. Access reporting will be available to list all users accessing data over time. This will be reported on quarterly.

Software Management

The following section details software management at NIESR.

Software Upgrades

35. Software must be kept up to date on the systems that NIESR use, including major versions and interim updates.
36. The exception to this is where a specific version of software must be used to analyse data and produce the results required by NIESR.
37. Incidences where this is the case must be clearly documented and approved.

Software Metering

38. NIESR monitors on software usage to demonstrate where software is installed and how often it is used.
39. NIESR licensing and usage to be reported on monthly and software installations to be reviewed
40. Users to have permission to install software with prior approval and this software will then be identified in the monthly software audits. Unapproved software will result in remedial action on the PC.
41. PC's categorised to store Protected or Confidential data may not have software installed without prior authorisation and agreement within the IT security framework. Software may not be installed unattended on these machines.

Anti-virus Software

42. Anti-virus software is installed on all systems within the NIESR environment and automatically kept up to date.

Email Management

43. When data is received by NIESR the acceptable movement of the data will be clearly defined. Data or the results generated by NIESR should never be emailed externally or internally unless expressly allowed.
44. All email transactions to be journaled for reporting purposes

Appendix 4: Behavioural Insights Team Data Security Policy

Separate document attached.

THE
BEHAVIOURAL
INSIGHTS TEAM

THE
BEHAVIORAL
INSIGHTS TEAM

The Behavioral Insights Team Data Security and Storage Policy

THE BEHAVIORAL INSIGHTS TEAM

Contents

THE
BEHAVIORAL
INSIGHTS TEAM

The Behavioral Insights Team Data Security and Storage Policy

This document outlines the Behavioral Insights Team's (BIT henceforth) protocol for managing data. It details both our general principles of data governance and the procedures to be followed by all users of data.

1. Governing Policy and General Principles

1.1 Objectives

This policy outlines data security and storage principles used by BIT when handling data provided by partner organizations. All protocols have been designed to ensure that any risks to data security are minimized and to a standard demanded by law -- and in accordance with data sharing agreements held by BIT.

In summary, this policy:

- Protects all identifiable information about people that participate in our studies;
- Sets the rules for expected behavior by users, BIT senior management and other BIT employees involved with data collection, storage or analysis;
- Explicitly defines the company's stance on data security;
- Minimizes risk.

1.2 Commitments

BIT is committed to protecting the security of its data and data systems in order to ensure that:

- The integrity of data is maintained, so that it is accurate, up to date and 'fit for purpose';
- Data is always available to those who need it and there is no disruption to the business of the company;
- Confidentiality and security is not breached, so that information is accessed only by those authorized to do so;
- The partner organization is comfortable with the use of data for a specific project by a specified team. This may involve criminal background checks for those team members with access to the data;
- The company meets its legal requirements;
- The reputation of the company is safeguarded.

In order to meet these aims, the company is committed to implementing security controls that conform to best practice. The company has also drawn up a number of different protocols in order to provide guidance on the practical aspects of data security and storage. The summary of these protocols can be found in section 2 of this document.

1.3 Data Protection Principles

In applying data protection principles to BIT's own work protocol, all employees should adhere to the following guidelines:

Only process accurate and relevant data. When processing personal data you must ensure that it is accurate, relevant and not excessive in relation to BIT's needs.

Ensure participant anonymity. Do not disclose any information (including giving references) about an individual identifiable in data to an external organization without first checking that the individual consents to such disclosure and the Head of Research has given permission.

Request permission if moving data. Any work concerning data that is undertaken outside the office requires the permission of the Head of Research. Under the very rare circumstances where this is granted, employees must be vigilant. Strict security measures must be applied to transportation and storage of all such data.

Store data safely and securely. Ensure that all data is kept secure, not only from unauthorized access, but from fire and other hazards.

Dispose of old data. Use a shredding service to dispose of any document containing personal data (electronic or otherwise) after two years of last expected use (or after the time specified in a data sharing agreement).

Use passwords. Apply password protection to computers and other data storage devices. When absent, ensure that the office door is locked and that your desk is kept clear of personal data.

Secure passwords. Do not make passwords for data available to unauthorized persons.

This is a general list of principles and not intended to be interpreted as a complete or comprehensive set of instructions. Please consult the detailed set of procedures in section 2 of this document for information on using or storing data.

1.4 Incident Response

The principles and procedures set forth in this document have been designed to minimize the risk of any lapses in data security to any data that the Team is responsible for.

Any and all breaches and foreseeable risks to data security should be reported to the Head of Research or, if not available, the next most senior member of BIT, as soon as possible.

All members of BIT are responsible for the security of the information that they come into contact through their work with the company. Failure to adhere to this policy may lead to action under BIT's formal Disciplinary Procedure.

2. Data Management

2.1 Receiving Data

There are a number of ways to send sensitive data to BIT in a secure fashion.

1. **Password protected options** - Passwords can be used to add an additional layer of security on files. BIT will only have one person with access to any password, and communication with any partner or client about the password should be made over the phone or in-person.
2. **Remove sensitive information** - In many cases, BIT does not need to have access to names, addresses, and other personally identifiable information. In these cases, BIT can advise on how to go about eliminating sensitive information from outgoing data, or remove the data immediately upon receipt.
3. **Accellion** - BIT has an account with Accellion, which offers a secure file transfer service and can handle large files. Permissions can be tailored to ensure that only BIT and you have access to specific files, and waterworks can be added to protect confidential information.
4. **In-person pick-up**: If rules and regulations do not permit sending data from from a certain machine, BIT can arrange an in-person visit to load the data onto an external storage device. BIT will make every effort to keep this data secure (e.g., password protected and encrypted).

This list is not intended to be comprehensive per se; if there are other data transfer services that a partner organization uses, BIT will discuss informal arrangements or a formal data sharing agreement.

2.2 Cleaning Data

Upon receiving new data, the line by line data should be inspected by a member of the Data Team for personal information. If new variables are to be derived based on this personal information (such as age from date of birth), this should take priority over all

other cleaning. After these variables are derived, variables containing any personally identifiable information should be dropped from the main dataset and replaced by an anonymous code. Which variables are dropped and why should be recorded in the data management appendices of the trial report. The cleaning of any dataset must be recorded in the data log.

2.3 Storing Data

If BIT receives data with identifiable or personal information, BIT will store the raw datasets, files, and logs--for STATA or any other statistical software package--on two external hard drives. The hard drives are physically stored in a locked cabinet and password protected. They do not leave the BIT offices unless it is absolutely necessary and there is explicit written permission from the Head of Research. If data requires enhanced security protection, as determined in collaboration with the partner organization, it is stored in a secure data room on a password-protected non-networked computer that only BIT researchers can access.

BIT will store cleaned data, without any personal or identifiable information, on a password protected shared drive.

2.4 Disposal of Data

BIT will retain all datasets for two years after their last expected use to ensure replicability of findings. At the end of two years (or after the specified date in the data sharing agreement), data will be permanently deleted from any and all drives.

Appendix 5: Data Sharing Agreement

BACKGROUND

In order to evaluate the Improving Working Memory randomised controlled trial it will be necessary for the University of Oxford project team (Oxford), participating schools, the National Institute of Economic and Social Research (NIESR) and the Behavioural Insights Team (BIT) to share data. This includes:

- data used to identify participating schools and pupils in the Department for Education's (DfE) National Pupil Database (NPD)
- outcome data obtained through assessment (mathematics assessments; working memory measures)
- teachers' assessments of pupils attention and behaviour in class
- Information on pupils' activities, including use of the online game.

These data will only be used for the purposes of the evaluation and will be treated with great care to achieve high levels of security. Further information on this process is provided below.

DATA SECURITY

Data transfer between schools, Oxford, NIESR & BIT

The project will involve transferring potentially sensitive pupil data between the schools, project team (Oxford) and evaluation team (NIESR/BIT). Such data must be transferred securely, meaning that the following process will be followed carefully.

Secure data may be transmitted via email, with the following standards applied. It will be stored using an encrypted Microsoft Excel (.XLSX) spreadsheet. The password to open, edit and re-save this encrypted file will be agreed in advance of transfer and will not be reused across different parties. These passwords will conform to the following standards and will never be shared via email:

- Minimum length: 8 characters
- Contains at least one uppercase letter
- Contains at least one lowercase letter
- Contains at least one number

Data may also be transferred physically, for example if collected as part of visits to schools for testing. Any potentially sensitive data will be stored on an encrypted USB flash drive when in transit. BIS use VeraCrypt encryption for USB flash drives; Oxford requires that confidential data must be encrypted, using AES 256bit encryption or stronger, when stored on mobiles devices or removable media.

As part of the application for access to the NPD, potentially sensitive data on participants will need to be transmitted to the DfE. This is likely to be done using the DfE's secure Key2Success service. Whatever form it takes, all relevant guidance from the DfE will be followed for this process. Matched, anonymised data will be transmitted back from the DfE to NIESR using the same process.

BIT will collect data on the attainment measures directly from the schools. Data collected from the schools by BIT's research assistants will be anonymised (and individuals pupils will be identified through the use of a unique case identifier) before being saved in electronic format and the hard copies will be returned to BIT's offices and stored in BIT's secure, locked data room. This process can be reflected in the MOUs between participating schools and the project partners. These data will be securely stored on BIT's secure database. Data transfer to NIESR/Oxford will follow the same process set out above.

After final completion of the project the data will be passed to EEF and/or its contractors for the purposes of contributing to the cross-project database. This data transfer will be carried out in line with the security procedures outlined above.

Data storage at NIESR

Data will be stored by NIESR using their secure network storage and handled according to NIESR's Data Security Policy (see document enclosed). The data will be treated as "Confidential" using NIESR's internal rating system, meaning that data are stored in an area that is only accessible to

users that are specifically allowed access to the data (this will be restricted to members of the evaluation team); the data will be kept encrypted when not in use. In addition, the NIESR network is fully protected at the perimeter by a firewall device. This prevents external traffic or connections into the NIESR network unless specifically allowed.

The data will be backed up to an internal storage platform, encrypted in transit, and encrypted while it is stored. We do not foresee the need to move the data onto physical media while at NIESR. Access to the data is automatically monitored to allow identification of individuals accessing the data and so that checks can be made that no unauthorised access has taken place. After completion of the project and publication of any related academic outputs, NIESR's copy of the data will be destroyed using PGP Shredder software, set to use 3 passes, which exceeds DoD 5220.22-M data destruction standards.

Data storage at BIT

BIT will ensure that:

- the Data will only be accessed by those who are part of the project on a need to know basis;
- all BIT analysts working on this project will have a cleared Disclosure and Barring Service (DBS) check in place;
- unauthorised staff and other individuals will be prevented from gaining access to the Data provided;
- data security risk assessments are performed for all data systems on a regular basis in order to identify key data risks and determine the actions required to keep those risks within acceptable limits;
- all computer systems and other data storage devices that contain personal or sensitive personal data are password protected;
- workstations / PCs are not left signed on when not in use;
- all disks, tapes, other removable media or printouts are locked away when not in use in Bits secure data room;
- no personal or sensitive data is transmitted via unencrypted email;
- no Data is left on public display in any form, with all staff member desks cleaned at the end of each day and sensitive material locked away safely;
- paper files are stored in BIT's secure data room (only accessible by a limited number of people in the research and evaluation team who have the door code)
- the office shredder or other contract shredding service is used to dispose of any document containing personal data (electronic or otherwise) after use;
- all datasets and do-files, for Stata or any other statistical software package, are stored on an encrypted, regularly backed up, team hard-drive;
- all members of staff adhere to these procedures and standards;
- sufficient training is provided to all staff members to ensure they understand the importance of data security and, in particular, exercise appropriate care when handling personal and sensitive information;
- failure to adhere to this above procedures and standards by any individual BIT staff member may lead to action under BIT's formal Disciplinary Procedure.

Data storage at Oxford

The Department of Education has an up-to-date information security policy which will be adhered to in relation to this project's data. All staff, students, visitors and collaborators using the Department's IT systems, data or any other information asset should follow the Department's Information Security Policy, the security policy references to ISO27002 (see document enclosed).

All confidential data will be stored securely; if a hard copy is kept, it will be stored in a locked cupboard in a locked room or, if stored electronically, data will be stored on departmental file servers attached to a corporate network and not on local hard drives. The server is backed up remotely to a server at the University IT Services. The PC where data will be processed is located in a locked room. The server where data will be stored is contained in a locked room. All of these locked rooms are within buildings only accessible via authorised swipe cards, and all access is logged on the access system. Also all external doors are video monitored 24 hours a day.

After completion of the project and publications, all media will be shredded and data held on the server will be deleted. We will securely erase using a utility called File Shredder. When the server is

retired from service the hard drives it contains will be physically destroyed so no data can be recovered from them. This is a service periodically provided by University IT Services who have access to a disk crushing device.

USAGE OF THE DATA

At no time will individual- or school-level data be disclosed to any third parties (with the exception of end of project transfer to EEF/its contractors as noted above). It will only be used for purposes connected with evaluation of this project including, but not specifically limited to:

- Checking randomisation has worked through analysing the average characteristics of individuals and schools in the treatment and control groups;
- Calculating the estimated impact of the project by comparing the outcomes of individuals in treatment and control schools.

This includes use of the data for academic publications by the project and evaluation teams, which will follow the same standards in terms of ensuring confidentiality and anonymity of participants.

MONITORING DATA/PROCESS EVALUATION

During the project the project team will be keeping in regular contact with participating schools (treatment and control groups). Where relevant, notes will be shared with the evaluation team for the purposes of the quantitative and process evaluations. The evaluation team will carry out data collection and analysis for process evaluation. Where relevant, information will be shared with the project team to support successful implementation. The project team will cooperate with the evaluation team to support the process evaluation (e.g. assisting with liaison with the schools to arrange research visits).

AGREEMENT

NIESR, BIT and the University of Oxford agree work collaboratively in the sharing of data for the success of this project and will follow the procedures outlined in this document when handling the potentially sensitive data included that will be shared as part of this project. Any actual or potential breaches will be notified to the relevant data controller.

Signed:

Maureen Cole-Burns
Chief Operating Officer
National Institute of Economic and Social Research

Nicky Kerr
Legal Counsel
Behavioural Insights Ltd.

Jo-Anne Baird
Director of the Department of Education
University of Oxford