Data Protection Policy
(GDPR)

Policy Version	Date Approved	Signed by Director	Signed by Executive Principal	Signed by School Lead
4.2	MAY 16			
4.2	FEB 18			
5.0	JUL 18			
5.1	AUG 18			

DATA PROTECTION POLICY

CONTENTS

1. INTRODUCTION

Nishkam School Trust (NST) has a commitment to protect personal data, alongside ensuring data is collected and used in a fair lawful manner.

NST collects and uses personal data regarding staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the trust to provide excellence in education and other associated functions.

Personal data is any information that relates to a living individual who can be identified from the information. Personal data can include information held in many formats including paper records, electronic systems, photographs, video clips (including CCTV), or sound recordings.

2. PURPOSE

This policy is intended to ensure that personal data is maintained accurately, kept up to date and secure in accordance with the Data Protection Act 2018 including the General Data Protection Regulation (GDPR), and other related legislation.

This policy covers all aspects of the use of personal data by schools in the Trust, this is referred to as "processing". Processing includes the collection, use, storage, sharing, management and disposal of personal data.

The Trust will only process personal data where it is necessary or where we are required to by law or regulation.

3. SCOPE

The Data Protection policy applies to all individuals involved with the collection, processing and disclosure of personal data. All NST employees (including Governors and Directors of the Trust and its member schools) working with personal data have a responsibility to ensure that they have sufficient awareness of requirements of the Data Protection Act 2018 and GDPR so that they are able to comply with the responsibilities related to processing individuals personal data.

Staff who have questions regarding this policy or require more detailed guidance are advised to contact their manager or the Head of Business Services.

4. ROLES AND RESPONSIBILITIES

NST is responsible for personal data relating to parents, pupils, staff, governors, directors, visitors and others, and therefore is a "data controller".

NST, as a Data Controller, is registered with the Information Commissioner's Office (ICO) our registration number is Z2743931.

The Trust issue a Privacy Notice to all pupils/parents and staff which summarises the personal information it uses, why it is held and the other parties to whom it may be passed on to. Privacy Notices are published on the school website in line with statutory guidance.

Information Governance refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and

future regulatory, legal, risk and operational requirements. Any complaints or concerns regarding the handling of data parties can be dealt with by emailing Nishkam School Trust at:

- enquiries@nishkameducation.org - for parents
- hr.enquiries@nishkameducation.org – for staff

Staff who believe that fellow colleagues are not complying with data protection laws and/or this Policy are encouraged to report this to the Data Protection Officer at DPO@nishkamschools.org or to the Principal/Headteacher

NST's Board of trustees has overall responsibility for ensuring that schools in the Trust academies comply with all relevant data protection obligations.

The Data Protection Officer (DPO) is responsible for monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide a termly report of their activities directly to the NST Trust Board and, where relevant, report to the board their advice and recommendations on data protection issues. The DPO is also the first point of contact for individuals whose data NST processes, and for the ICO. Our DPO is provided by Services4Schools Ltd and is contactable at DPO@nishkamschools.org.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with the relevant school in the first instance, or contact our DPO.

Alternatively, you can contact the Information Commissioner's Office direct at https://ico.org.uk/concerns/

The Information Commissioners Office (ICO) is the supervisory authority for data protection in the UK. It has extensive powers, including the ability to impose civil fines, instruct the ceasing of processing, undertaking investigations into possible data breaches or unlawful processes.

NST will adhere with any request from the ICO to comply with instruction it issues in relation to the Data Protection Act 2018/GDPR and ensure that any organisations who process data on behalf of NST comply with the ICO if required to do so.

5. DATA PROTECTION ACT 2018/GDPR

The Data Protection Act 2018 and GDPR establishes six principles that NST fully endorses and adheres to at all times.

Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6. POLICY

NST is committed to maintaining the above principles at all times. Therefore the Trust and its member schools will:

- inform individuals why the information is being collected when it is collected;
- inform individuals when their information is shared, and why and with whom it was shared;
- check the quality and the accuracy of the information it holds;
- ensure that information is not retained for longer than is necessary;
- ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- share information with others only when it is legally appropriate to do so, or where an appropriate consent has been established;
- set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- uphold the rights of individuals under GDPR
- ensure our staff are aware of and understand our policies and procedures.

It is the responsibility of all employees of NST to take care when processing personal data (collecting, managing, storing, sharing, transferring and destroying) to ensure it cannot be accessed by anyone who does not:

- have appropriate permission, or explicit consent to access that data
- need to have access to that data as a result of a statutory requirement (ie safeguarding procedures)

NST Any loss or misuse of personal data can have serious effects for both individuals with personal liability and / or institutions concerned, as it can bring the school into disrepute.

NST will regard any unlawful breach of any provision of the DPA/GDPR by any individual, as a serious matter which will result in disciplinary action. Any employee who breaches this policy will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

All data protection incidents must be reported immediately to the Prinicipal/Headteacher

7. SECURE STORAGE OF AND ACCESS TO DATA

NST will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

All staff should ensure that:

- Personal data is only accessible on school devices which have secure access
- Access is controlled; users will only be granted a given level of access data dependent on his/her role

Additionally staff must abide by the guidelines for confidentiality and data security within the NST policy for 'Telecommunications and Use of Computers'.

The nominated 'Lead for Data Protection' at each school locally will ensure that data protection procedures are appropriate and adequate.

Deliberate unauthorised access to, copying, disclosure, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

8. SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The school recognises that personal data may be accessed by users out of school, or transferred to the DfE, Local Authority or other multi-agency organisations. In these circumstances:

- Users may not remove or copy RESTRICTED or personal data from the school or authorised premises. If there is a circumstance that may require this permission must be sought by staff from the Principal/Headteacher who may consult with the DPO before making a decision.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members or friends) in or out of school
- The Trust will ensure that all portable and mobile devices, including media, used to store and transmit personal information will be installed with approved encryption software

Any loss or inappropriate disclosure of personal data must be reported immediately to the Headteacher and/or the DPO, failure to do so will constitute misconduct and may result in disciplinary measures.

9. RETURNING OF ICT EQUIPMENT

The Headteacher/Head of Business Services will maintain an inventory and will audit all school ICT equipment such as desktop and laptop computers and all portable devices.

Members of staff who are leaving must return all personally-issued ICT equipment to the Headteacher/Head of Business Services and sign a declaration confirming they have returned all school equipment and property.

10. ACCESS TO PERSONAL DATA AND THE DISCLOSURE OF EDUCATION RECORDS

There are two distinct rights of access to personal data held by schools:

- Under the Data Protection Act 2018/GDPR any individual has the right to make a request to access the personal data held about them. This is commonly referred to as a Subject Access Request
- The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005 (Pupil Information Regulations).

These procedures relate to subject access requests made under the Data Protection Act 2018/GDPR.

1. Requests can be made in writing to the school marked for the attention of the Data Protection Officer, by email to DPO@nishkamschools.org, or verbally, but you may asked to provide supplementary information in writing to confirm the detail of any request made.

   If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

   - passport
   - driving licence
   - utility bills with the current address
   - Birth/Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

   (This list is not exhaustive).

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school will not usually charge for Subject Access Requests, but in some circumstances may make a charge for the provision of information, dependent upon the following:
   - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
   - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 30 days **(not working or school days but calendar days, irrespective of school holiday periods)**. If a request is deemed excessive or unfounded an additional time period of up to two months may be applied to dealing with a request, but in the this case the person who has made the request will be notified.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore **all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another organisation where there is an expectation of confidentiality, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent will be sought. A response will still be made within the 30 day statutory timescale, but may not include third party information where consent has not been provided.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another will not be disclosed, or any information that would reveal that the child is at risk of abuse, or information relating to court

proceedings.

9. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.

10. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

NST will also keep curricular and educational records for each pupil, disclose these records to parents and pupils, report at least annually to all parents on their child's progress and attainment and transfer pupil information and educational records as a pupil changes school.

11. RIGHTS OF INDIVIDUALS

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it though our Privacy Notices, individuals also have a number of other rights in relation to their personal data. For example, they can ask NST to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override NST's legitimate grounds for processing data (where NST relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful;
- Prevent use of their personal data for direct marketing;
- Stop processing or erase data which has been justified on the basis of public interest grounds;
- Provide a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- Refrain from taking decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress, unless this is being done in good faith in line with NST's Safeguarding & Child Protection procedures;
- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO at dpo@nishkamschools.org, or by post to the relevant school, marked for the attention of "The Data Protection Officer".

12. INFORMATION SHARING

Information sharing is a key element of safeguarding children and young people. NST will explain to students and their families what and how information will or could be shared, with whom and why, and also seek additional consent as required.

It is the responsibility of teachers to ensure appropriate information is shared effectively, appropriately, legally and professionally. Personal data must only be shared with other professionals, relevant support staff or other teachers for genuine purposes.

Whilst parents have a right to expect that personal information they share with NST will be

regarded as confidential, there are certain circumstances when information can be shared without parents' consent, such as when;

- there is evidence that the child is suffering, or is at risk of suffering, significant harm
- there is reasonable cause to believe that a child may be suffering, or at risk of suffering significant harm
- failing to do so would put a pupil at increased risk of significant harm; or
- it would undermine the prevention, detection or prosecution of a serious crime

13. RETENTION OF DATA

The school will comply with the requirements for the safe destruction and disposal of personal data when it is no longer required. No documents will be stored for longer than is necessary; this is to adhere to any legal, regulatory or specific business justification.

NST has a retention schedule which services as a guide to how long records that contain personal data should be kept for. Staff at all school should refer to the retention schedule before destroying or disposing of records (live or archived)

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records and overwrite or delete electronic files.

We may also use a third party to safely dispose of records on NST's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. DATA BREACHES

NST will make all reasonable efforts to ensure that the personal data it is responsible for processing is not lost, shared inappropriately or unlawfully processed in any other way. If this does occur it is recognized as a "breach".

All breaches or suspected breaches of personal data should be reported immediately to the Data Protection Officer.

When appropriate, the DPO will report the data breach to the ICO within 72 hours.

A breach could include (but not limited to):

- An email containing personal data of staff or pupils being sent to an incorrect recipient
- Paper records of pupils or staff accessed/read by unauthorized person
- Pupil records being shared inappropriately with an external agency
- Safeguarding information being made available to an unauthorised person
- The theft of or loss of a school laptop or memory stick containing non-encrypted personal data about pupils and/or staff
- Paper records of NST pupils or staff being lost by a third party

15. MONITORING AND REVIEW

A general review of the policy and compliance with legislation will take place every 2 years. Changes to the policy will be made earlier where necessary.

Appendix 1 –Data Protection Guidance for Staff

Personal data: any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information.

Sensitive personal data: includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals.

Paper Records

- Keep paper records containing the personal data of students or staff secure at all times, in the classroom, around school, during transit and at home.
- Do not leave paper records sensitive information unattended; where possible store it in lockable drawers/cupboards.
- All paper based school trip information, medical advice contact addresses, allergies etc. must be returned to the school at the end of the trip for secure filing or shredding.
- Keep a clean desk, don't leave sensitive information on view for students / other staff to read.
- Collect printing that contains personal data immediately - Do not use student to collect sensitive information from printers / copiers.
- Dispose carefully of any paperwork that contains personal – use shredders / secure bins.

Devices & Applications

- Ensure all school devices are kept secure at all times, in the classroom, around school, during transit and at home.
- Ensure all devices are logged off or locked when they are left unattended.
- If you are using a mobile device (phone) to access work email or network resources, ensure that the device is password protected.
- Only use school devices to take and record student images.
- Do not use personal devices to access, view or store school-related personal data.
- All external USB Drives used for school purposes must be encrypted.
- Do not acquire or use applications, software or websites requiring information on pupils/staff data without prior authorisation by the school.
- When working with sensitive data, do not position screens where they can be read by other people.

Wifi, Access & Downloading

- Do not log on to public Wi-Fi networks or use public computers whilst working with school-related personal data.
- Access data remotely, instead of taking it off-site, using secure systems approved by the ICT Support team.
- Do not save or download school-related data onto personal devices unless first authorised by the school.
- Ensure that any downloaded personal data stored on a shared network drive or the cloud is password protected and permanently deleted when is no longer required.

Passwords

- Ensure all passwords are kept secure and meet the complexity requirements when they are changed or created. Passwords must be at least 8 characters long and contain characters from three of the following four categories:

  1. *Uppercase characters of European languages*
  2. *Lowercase characters of European languages*
  3. *Base 10 digits (0 through 9)*
  4. *Nonalphanumeric characters:* ~!@#$%^&* -+=`|\(){}[]:;'"<>,.?/

- Do not share your passwords with anyone or write them down.
- Do not save passwords in web browsers if offered to do so.

E-mails

- Email accounts issued by the school are not private property and form part of the schools administrative records. The content of emails may be disclosed to individual or outside agencies, as required by the Data Protection Act 2018.
- Do not use personal (non-school provided) email accounts to conduct school business. A school email account should be used for school business and not for personal correspondence or other purposes.
- Do not open any email attachments sent by unrecognised senders.
- Do not send by email any material that is viewed as highly confidential or contains personal data, unless is encrypted/password protected. In such cases the encryption key/password must be communicated by other means (in person or over the phone).
- Ensure that emails are being sent to the intended recipient by double checking their email address before sending.
- Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers.

Displaying / Presenting Data

- Keep personal data anonymous if possible, for example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to.
- Be mindful what personal/sensitive data may be on display in class when visitors, agencies and parents are accessing rooms.
- Think before you put information up on the wall if you may need consent from the parent or pupil or if there might be a safeguarding risk in displaying it.

Reminders

- Remember that data protection laws DO NOT stop you from reporting safeguarding concerns. You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this.
- If you have to share highly personal or confidential information, do so in person, over the phone or via a secure managed file transfer.
- Read and understand all of the school's policies on data protection.
- Only keep data for as long as is needed. If you are not sure how long to keep data for, check the school retention policy.

- Speak to the DPO / Headteacher if:
  - You have any concerns at all about keeping personal data safe
  - You're introducing a new process or policy that involves using personal data
  - Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information
- Contact the DPO / Headteacher immediately if you think personal data has been lost, stolen or wrongly disclosed.

STAFF NAME: _____

SIGNATURE: _____

DATE: _____

Appendix 2 - NST process for breach management (September 2018)

Summary of Key Responsibilities in the event of a breach:

Principal/Headteacher (Local School)

- - Inform the CEO & Chair of Governors about any potential breaches immediately
- - Co-ordinate activities to contain and minimise the breach
- - Responsible investigation and recording of breach incidents and liaising with DPO for advice
- - Deciding in conjunction with CEO, Chair of Governors and DPO if incident will be reported to the ICO
- - Provide a detailed report of lessons learned and share with Link Governor & Governing Body
- - Appoint Data Protection Lead for school and ensure he/she has relevant training for to assist in developing a data protection culture throughout organisation and help prevent breach

Data Protection Officer (DPO) – Trust Level

NST DPO services will be provided by Services for Schools (S4S) who can be contacted via DPO@nishkamschools.org

- Production of Risk Register for NST (including all individual schools)
- Overall Management of compliance for NST
- Production of termly Directors reports regarding GDPR
- Provide advice and guidance on Issue/Breach Management to individual schools within the Trust
- Reporting of issues/breaches to ICO (in agreement with Principal/Headteacher & CEO)

Data Protection Lead (DPL) – Local School Level

- - First point of contact in school to provide general advice to staff on Data Protection, co-ordinate data protection training for staff and foster a culture for data protection within the school
- - Has in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- - Ensures the schools IAR (Information Asset Register) is updated and maintained
- - Analyses and checks the compliance of data processing activities (including agreements with data suppliers)
- - Provide the information required for the termly update to the Link Governor for Data Protection

What is a Breach?

A Breach of the Data Protection Act 2018 or GDPR is where personal data has been accidentally or unlawfully processed. This may include where an individual's personal data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

What will happen next

- On finding or causing a breach, or a potential breach, the staff must immediately inform both:
  1. The Principal/Headteacher and Data Protection Lead (DPL) unless the disclosure is potentially a confidential whistleblowing matter;
  2. Notify the Data Protection Officer via email at DPO@Nishkamschools.org.
- The school assisted by the DPO will investigate the alleged data breach and determine whether a breach has occurred.
- The Principal/Headteacher should inform the CEO and Chair of Governors of any potential breach immediately whilst it is being investigated.

- The DPO will also alert the relevant headteacher and/or the CEO of the Trust to ensure they are aware of the potential breach whilst it is investigated.
- The school will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO, relevant staff members e.g. DPL where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- Principal/Headteacher and DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Principal/Headteacher, CEO and Chair of Governors in conjunction with the DPO will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the School and DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the breach should be reported to the ICO..
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored in as part of the relevant Information Asset Register (IAR) and risk register (maintained by the DPL in each School).
- Where the ICO must be notified, the DPO will do this within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO and relevant school will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will assist the school in the process of informing, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The school will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO in conjunction with the DPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored on each base academy's data audit spreadsheet.
- In the case of a reportable breach, the DPO and relevant Principal/Headteacher and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. In these circumstances, the Principal/Headteacher will be responsible for sharing this information to the CEO at the Trust SLT meetings, so that lessons can be learnt and appropriate interventions or training put in place.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- The school will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted