the beckmead trust

nurture • sustain • grow

Data Breach Policy

Approved on:	16 July 2026
Approved by:	Board of Trustees
Last reviewed on:	July 2026
Reviewed by:	Dee Fullerton
Next review due by:	July 2027

Summary of Changes

[Use the table below to insert any changes made to the document since the last approval. Please delete text as appropriate]

Date	Updates	Page No.

Contents

1. Introduction

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

2. Definitions

Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Special Category Data	Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or

	religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data or special category data transmitted, stored or otherwise processed.
Data Subject	Person to whom the personal data relates.
ICO	The ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.
Data Protection Officer (DPO)	The person we appoint from time to time to lead the development and implementation of our data protection and compliance with the UK GDPR and other applicable.

3. Responsibility

The Head Teacher has overall responsibility for breach notification within the School. In Central Services the Director has this responsibility. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches. These senior members of staff are responsible for ensuring their local data breach log is kept uptodate and available for inspection and audit.

All breaches must be reported immediately to the Head Teacher and the Director of Compliance (dpo@beckmeadtrust.org). In the absence of the Head Teacher, please contact the Director of Compliance immediately.

The Director of Compliance with the Trust Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the Director of Compliance with any questions about the operation of this policy or the UK GDPR, or if you have any concerns that this policy is not being or has not been followed.

4. DPO Contact Details

The DPO's contact details are set out below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1, then option 1

5. Security and Data Related Policies

All schools within the Trust must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. In particular, staff should refer to the following policies that are related to this Data Breach Policy: -

- The Trust Digital Policy
- Trust Data Protection Policy
- Data Retention Policy
- Trust Staff Code of Conduct
- Trust Freedom of Information Policy
- Trust CCTV Policy

These policies are also designed to protect personal data and can be found on the local school landing page.

6. Data Breach Procedure

What is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored for example, loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example, sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it;
- Alteration of personal data without permission;
- Loss of availability of personal data.

When does it need to be reported?

The Trust/School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example, through the release of non-public identifiers such as passport details); and
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Report the breach immediately to your Headteacher and your line manager
- Complete a data breach report form (Appendix 1);
- Email the completed form to the Director of Compliance via dpo@beckmeadtrust.org.

Where appropriate, you should liaise with your line manager about completion of the data report form. However, this may not be appropriate or possible, e.g., if your line manager is aware of the breach and instructed you not to report it, or if they are simply not available. In these circumstances, you should submit the report directly as above, without consulting your line manager. Breach reporting is encouraged throughout the Trust/School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Headteacher or Director of Compliance via dpo@beckmeadtrust.
Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Director of Compliance will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, The Director of Compliance will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:-

- Where possible, contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

Containment and Recovery

The Director of Compliance, with the Headteacher or Director, will identify how the breach occurred and take immediate steps to stop to minimise further loss, destruction or unauthorised disclosure of personal data.

The Director of Compliance, with the support of the DPO and Headteacher, will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, the Director of Compliance, with the support of the DPO, will notify the Professional Indemnity Insurer and/or cyber insurer and/or crime insurer], as the insurer can provide access to data breach management experts.

7. Notifying the ICO

The Director of Compliance, following discussion with the DPO, will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e., it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption will be to report it (see below).

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

If the Trust/School is unsure whether to report, the presumption should be to report. The school will take into account of the factors set out below:

8. The potential harm to the rights and freedoms of data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

- Exposure to identify theft through the release of non-public identifiers, e.g. passport number;
- Information about the private aspects of a person's life becoming known to others, e.g. financial circumstances;

The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

The volume of personal data

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned; and
- There is a real risk to individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

The sensitivity of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable;
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

8. Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Director of Compliance will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, The Director of Compliance will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Trust/School will consider alternative means to make those affected aware (for example, by making a statement on the School website).

9. Notifying the Police

The Trust/School will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the Trust/School will notify the police and/or relevant law enforcement authorities.

10. Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example:

- The Information Commissioners Office (ICO);
- Affected data subjects;
- Insurers;
- Parents;
- Third parties (for example, when they are also affected by the breach);
- Local authority;
- The police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive and confirmation of parties to be notified will be discussed with the Director of Compliance.

11. Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The Trust/School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. The Trust/School will identify ways to recover, correct or delete data (for example, notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e., the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation, two factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

12. Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;

- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

13. Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to The Director of Compliance or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

14. Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide regular training to staff:

- At induction;
- When there is any change to the law, regulation or our policy;
- When significant new threats are identified; and
- In the event of an incident affecting our school.

The School will ensure that staff are trained and aware of the need to report data breaches and to ensure that they know how to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

15. Record Keeping

The School and/or Directorate log must be updated with details of all data breaches whether the breach is reportable to the ICO or not. These records must be kept uptodate at all times and available for inspection.

16. Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

Appendix 1 - Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Director of Compliance via the dpo@beckmeadtrust.org email address using the form in **Appendix 2**
- The reported breach will be investigated to determine whether a breach has occurred. As part of the the consideration it will need to be ascertained whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
    - Made unavailable, with a significant negative effect on individuals
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the Director of compliance will alert the Headteacher and the Chair of Governors.
- The Headteacher with the Director of Compliance will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help with this where necessary. The Head Teacher and Director of Compliance should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO and Director of Compliance in discussion with the Headteacher will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will advise the Director of Compliance and Headteacher whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool .
- The Director of Compliance 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 are stored centrally by the Director of Compliance.
- Schools will ensure their local records for all breaches are stored electronically and available for inspection
- Where the ICO must be notified, the Director of Compliance will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the following will be 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 name and 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 those taken to mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the Director of Compliance will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The remaining information will be submitted as soon as possible
- Where the school or Directorate is required to communicate with individuals whose personal data has been breached, they will be advised in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and 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 those taken to mitigate any possible adverse effects on the individual(s) concerned
    - Any clear and specific advice on how the individuals can protect themselves, and what the school is willing to do to help them
- The Director of Compliance, on advice from the DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- Each school or Directorate will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts, including the cause
    - Effects
    - Action taken to contain it and make sure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be securely stored on the school system with restricted access.

- The Director of Compliance and Headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible
- The Director of Compliance and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to occur, 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.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

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 and immediately inform their Headteacher or Director.
- Members of staff who receive personal data sent in error must alert the sender and email the dpo@beckmeadtrust as soon as they become aware of the error.
- External parties who received personal data sent in error from the Trust can email the us directly via dpo@beckmeadtrust. Alternatively the can email our dpo via dataservices@judicium.com
- If the sender is unavailable or cannot recall the email for any reason, the Headteacher or deputy will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, contact the Director of Compliance to discuss whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Director of Compliance will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The Director of Compliance will arrange for an internet search, where appropriate, 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.

- If safeguarding information is compromised, the designated safeguarding lead and Head teacher will be and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other examples of breaches could be

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 2 – Data Breach Report Form

Beckmead School Name - Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- Complete this form; and
- Email or deliver it to dpo@beckmeadtrust.org ensuring that you mark your email as urgent, with the subject 'Data Breach'. Notify your headteacher and Line Manger.

Time is of the essence with data breaches. You must submit this report as soon as you know or suspect there has been a data breach.

Do not delay to satisfy yourself whether a data breach has definitely happened and do not contact any individuals who may be affected by the data breach. The Director of Compliance] along with DPO, will investigate the potential breach and take necessary actions.

Name and contact details of person notifying the actual or suspected breach	*[Insert name and contact details]* *If you wish to submit an anonymous report, leave this section blank*
Department/manager	*[Insert department from which the report emanated and the relevant manager]*
School Site address	
Location on site of breach	
Date of actual or suspected breach	*[Insert date]*
Date of discovery of actual or suspected breach	*[Insert date]*
Date of this report	*[Insert date]*
Summary of the facts	[*Provide as much information as possible – including the amount, sensitivity and type of data involved*]
Cause of the actual or suspected breach	*[Provide a detailed account of what happened]*
Is the actual or suspected breach ongoing?	Yes ☐ No ☐ Not known ☐
Who is or could be affected by the actual or suspected breach?	*[Include details of categories and approximate number of data subjects concerned]*
Are you aware of any related or other data breaches?	Yes ☐ No ☐ [*If yes, provide more details*]