Bridge Academy Trust

DATA PROTECTION POLICY

January 2023

CHECKLIST

Please put an x in the box when done

Set up draft policy with watermark	☒
Ensure footer says draft	☒
Date on front and footer is date the policy comes into action	☒
Committee taking to – include date	☒
Summary of changes – to be brief	☒
When updated save in DRAFT AWAITING FORMATTING	☒
Email Clerk when updated	☒

DOCUMENT FORMATTING

Please send to Clerk to format

Front page margins – Top & bottom 1.7, left & right 2	☒
Front page title – Arial 26, space under then date	☒
Headings – Arial 18, bold, capitals, border (thin line top, thick line bottom)	☒
Subheadings – Arial 14, bold, border (single thin)	☒
Font - Arial 11	☒
Margins – Front page – Top & bottom 1.7, L&R 2	☒
Margins – Main Policy – Top 2, Bottom 2.54, L&R 2	☒
Main Number Margins – 0.00, 1.5	☒
Bullet Points Margin – 1.75, 2.25	☒
Sub-numbers Margin – 1.75, 3 (9pt)	☒
Bullet Points & Sub-numbers – paragraph 6pt	☒
Footer – Arial 10	☒
When formatted save in Draft for HT MEETING	☒

Agenda

To add a brief explanation:

Complete re-write will require a complete review	☒
Minor changes (spelling/ process etc.)	☐
No changes	☐

When a policy is ready for committee:

Consultation with Headteacher Group/ Trustees	☒

Once approved – Compliance Director to:

Remove reference to Draft watermark/ footer	☒
Ensure correct date – front and footer	☒
Save in to CURRENT under Clerk	☒
Add to website as appropriate	☒
To go on newsletter (liaise with Chief Officer PA) "Following the recent Policy Review Committee these policies were approved and can be found on 'staff portal'/ BAT website"	☒
SharePoint - Archive old policy! 1st September 2020	☒

Ensure the following:

Employees
Head of School
Students

Date of Draft Policy:	June 2022	
Date last reviewed by Trustees; Frequency of review:	June 2020 3 years	
Consultation with Staff Required:	Yes ☐	No ☒
Period of Consultation (if required):	From N/A	To N/A
Trust Committee Reviewing Document:	Full Board of Trustees	
Date of Board of Trustees Meeting at which Policy Approved (if required):	TBC	
Date of Adoption of Policy:	1 January 2023	
Date Policy available on Central Area/www (if appropriate):	1 January 2023	
Reviewer:	Data Protection Officer (DPO)	
Advice From:	GDPiRS	

Summary of changes

Reference to data protection legislation throughout.

2.1 addition of other policies

Appendix 2 added

Contents

INTRODUCTION

1.1 Bridge Academy Trust (the Trust) is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR and any other data protection legislation.

1.2 The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools, and educational bodies, and potentially children's services.

1.3 This policy is in place to ensure all staff/Trustees and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the data protection legislation. Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies.

LINKS TO OTHER POLICIES

2.1 This Data Protection Policy is linked to the following policies and documents and should be referred to as necessary:

- CCTV Policy
- ICT Acceptable Use Policy (Staff)
- IT Security Policy
- Staff Code of Conduct

DEFINITIONS

3.1 Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. The Trust is the Data Controller and staff within the Trust control data on behalf of the Trust.

3.2 Trust Data Processor means an employee of the Data Controller (Bridge Academy Trust).

3.3 Data Processor in relation to personal data, means any person/company (other than an employee of the Trust) who processes Data on behalf of the Data Controller e.g. Capita (third party).

3.4 Personal Data means any information relating to an identified or identifiable natural person.

3.5 Sensitive Data means any information that is clearly about a particular person.

3.6 Confidential papers means documents that should be kept private and not intended for common knowledge.

3.7 DPO means Data Protection Officer who is employed by the Trust to oversee data protection.

LEGAL FRAMEWORK

4.1 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018

4.2 This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'

APPLICABLE DATA

5.1 E-mails, documents, letters etc. that hold personal data are subject to data protection legislation. Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

PRINCIPLES

6.1 In accordance with the requirements outlined in the relevant data protection legislation, personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.
- will only be processed for specified, explicit and legitimate purposes which will be adequate, relevant, and limited to what is necessary in relation to the purposes for processing.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
- kept in accordance with the Records Management Policy.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or destruction or damage.

ACCOUNTABILITY

7.1 The Trust will implement appropriate checks to measure and demonstrate that data is processed in line with the principles set out in the data protection policy.

7.2 The Trust will provide comprehensive, clear, and transparent privacy policies.

7.3 Individual schools must keep internal records of the school's processing activities maintained and up to date:

- Data Asset Register
- Legal binding contracts
- Subject Access Requests

7.4 Each school must implement measures to:

- Data minimisation - only hold data for the use originally stated and only use further if essential for reasons that are clearly stated in advance
- Data transparency – assurance that data being reported are accurate and coming from official source. Data transparency is also the ability to easily access and work with the data no matter where data is located or what application has been used.
- To liaise with the DPO to continuously improve procedures as and when issues/concerns are raised.

7.5 Within the Trust with guidance from the DPO data protection impact assessments will be used where appropriate. Data impact assessments (DPIAs) helps identify and minimise risks that result from data processing.

DATA PROTECTION OFFICER (DPO)

8.1 A DPO will be appointed by the Trust in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor within the Trust compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

8.2 The individual appointed as DPO will have professional expertise and knowledge of data protection law, particularly that in relation to schools.

8.3 The DPO will report to the Director of IT.

8.4 The DPO will operate independently and will not be dismissed or penalised for performing their task.

LAWFUL PROCESSING

9.1 Under the GDPR, data used will be lawfully processed if the consent of the data subject has been obtained or processing is necessary for:

- compliance with a legal obligation.
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- for the performance of a contract with the data subject or to take steps to enter a contract.
- protecting the vital interests of a data subject or another person.
- for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

9.2 Sensitive data will only be processed if explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law, processing relates to personal data obviously made public by the data subject or processing is necessary for:

- carrying out obligations under employment, social security or social protection law, or a collective agreement.
- protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- reasons of substantial public interest on the basis of EU or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional.
- reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

9.3 Where the school relies on:

- ‘performance of contract’ to process a child’s data, the school considers the child’s competence to understand what they are agreeing to, and to enter into a contract.
- ‘legitimate interests’ to process a child’s data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.

CONSENT

10.1 Consent must be a positive indication not silence.

10.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

10.3 Where consent is given, a record will be kept documenting how and when consent was given.

10.4 The school will ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, DPO must be advised and processing must cease.

10.5 Consent can be withdrawn by the individual at any time.

10.6 Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

10.7 In all other instances with regards to obtaining consent, an appropriate age of consent will be considered by the school on a case-by-case basis, taking into account the requirements outlined in 7.2.

SHARING DATA WITHOUT CONSENT

11.1 The school may share information without consent in specific circumstances. To determine whether information can be shared with consent, the school will identify one of the other lawful bases for processing:

- contract – the processing is necessary for a contract held between the school and individual, or because the individual has asked the school to take specific tests before entering into a contract.
- legal obligation – the processing is necessary for the school to comply with the law (not including contractual obligations).
- vital interests – the processing is necessary to protect someone from risk to life or harm.
- public task – the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
- legitimate interests – the processing is necessary for the school's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

11.2 Where the school is able to justify one of the lawful bases outlined in 7.1, an exemption applies, or there is a requirement under another law, information may be shared without consent.

11.3 Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

THE RIGHT OF ACCESS

12.1 Individuals, including children, have the right to obtain confirmation that their data is being processed.

12.2 Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Subject access requests are to be requested via DPO.

12.3 The school will verify the identity of the person making the request before any information is supplied.

12.4 A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

12.5 Where a SAR has been made electronically, the information will be provided in a PDF (Portable Document Format) file, freely available to be read through Adobe.

12.6 Where a request is obviously unfounded, excessive or repetitive, a reasonable fee will be charged.

12.7 All fees will be based on the administrative cost of providing the information.

12.8 All requests will be responded to without delay and at the latest, within one month of receipt.

12.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

12.10 Where a request is obviously unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12.11 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

THE RIGHT TO RECTIFICATION

13.1 Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

13.2 Where the personal data in question has been disclosed to third parties, the Trust/school will inform them of the rectification where possible.

13.3 Where appropriate, the Trust/school will inform the individual about the third parties that the data has been disclosed to.

13.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

13.5 Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

THE RIGHT TO ERASURE

14.1 Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

14.2 Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

14.3 The right to erasure does not apply and the school/ Trust retains the right to refuse a request for erasure if the data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

14.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and then later request erasure of the data, regardless of age at the time of the request.

14.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves a disproportionate effort to do so.

14.6 Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

THE RIGHT TO RESTRICT PROCESSING

15.1 Individuals, including children, have the right to block or suppress data controller processing of personal data.

15.2 In the event that processing is restricted, the Trust Data Processor will store the personal data and inform the DPO, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

15.3 The Trust Data Processor will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust Data Processor has verified the accuracy of the data.
- Where an individual has objected to the processing and Trust Data Processor with guidance from the DPO is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead.
- Where the Trust Data Processor no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

15.4 If the personal data in question has been disclosed to third parties, the Trust Data Processor will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

15.5 The Trust Data Processor will inform individuals when a restriction on processing has been lifted.

THE RIGHT TO DATA PORTABILITY

16.1 Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

16.2 Personal data can be easily moved, copied, or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

16.3 The right to data portability only applies in the following cases:

- to personal data that an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means

16.4 Personal data will be provided in a structured, commonly used, and machine-readable form.

16.5 The Trust Data Processor will liaise with the DPO and provide the information free of charge.

16.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

16.7 The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.8 In the event that the personal data concerns more than one individual, the DPO will consider whether providing the information would prejudice the rights of any other individual.

16.9 The DPO will respond to any requests for portability within one month.

16.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

16.11 Where no action is being taken in response to a request, the DPO will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

THE RIGHT TO OBJECT

17.1 The Trust Data Processor with guidance from DPO will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

17.2 Individuals, including children, have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest
- direct marketing
- processing for purposes of scientific or historical research and statistics

17.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- an individual's grounds for objecting must relate to his or her situation.
- the Trust Data Processor will stop processing the individual's personal data unless the processing is for the establishment, exercise, or defence of legal claims, or, where the Trust Data Processor can demonstrate compelling legitimate grounds for the processing to the DPO, which override the interests, rights and freedoms of the individual.

17.4 Where personal data is processed for direct marketing purposes:

- the Trust Data Processor will stop processing personal data for direct marketing purposes as soon as an objection is received.
- the Trust Data Processor cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

17.5 Where personal data is processed for research purposes:

- the individual must have grounds relating to their situation in order to exercise their right to object.

- where the processing of personal data is necessary for the performance of a public interest task, The Trust is not required to comply with an objection to the processing of the data.

17.6 Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

AUTOMATED DECISION MAKING AND PROFILING

18.1 Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

18.2 The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

18.3 When automatically processing personal data for profiling purposes, the Data Controller will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

18.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Data Controller has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of EU/Member State law.

PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

19.1 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust data protection obligations and meeting individuals' expectations of privacy.

19.2 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

19.3 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

19.4 The Trust/school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes.

- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An outline of the risks to individuals;
- The measures implemented in order to address risk.

19.5 Where a DPIA indicates high risk data processing, the school will consult the DPO to seek his/her opinion as to whether the processing operation complies with the GDPR.

DATA BREACHES

20.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

20.2 Headteacher/Head of School will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

20.3 Where a definite/possible breach of data defined in point 18.1 the DPO will be informed.

20.4 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis by the DPO.

20.5 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.
- The name and contact details of the DPO.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

20.6 Failure to report a breach when required to do so may result in Bridge Academy Trust being fined and disciplinary action for the individual concerned.

20.7 The DPO must be informed as soon as a Data Breach has been identified via email at dpo@bridgeacademytrust.org. Please see Appendix A.

DATA SECURITY

21.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

21.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

21.3 Digital data must be coded, encrypted or password-protected, both are required on a local hard drive.

21.4 No Trust/ school data is to be stored on removable storage (e.g. memory stick or portable hard drive). Use of removable storage will be authorised by the DPO on a case-by-case basis. If the DPO has authorised the use of removable storage these devices must be encrypted by the Trust's IT Team.

21.5 Portable devices (such as, but not limited to laptops or iPads), the data must be encrypted, and password protected.

21.6 Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate communication.

21.7 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

21.8 When sending confidential information by fax, staff will always check that the recipient is correct before sending and alerting the recipient prior to sending.

21.9 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff must take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

21.10 Before sharing data, all staff members will ensure:

- They are allowed to share it
- That adequate security is in place to protect it
- Who will receive the data has been outlined in a privacy notice

21.11 Under no circumstances are visitors (non-employees) allowed access to confidential or personal information unless instructed by the DPO. Visitors to school areas containing sensitive information are supervised at all times.

21.12 The physical security of the Trust/school buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

21.13 The Trust takes its duties under the data protection legislation seriously. An unauthorised disclosure or wilful breach of data protection protocol may result in disciplinary action.

PUBLICATION OF INFORMATION

22.1 The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

22.2 When uploading information to the school website, staff are considerate of any data that provides information about other data (metadata) or deletions which could be accessed in documents and images on the site.

CCTV AND PHOTOGRAPHY

23.1 The Trust understands that recording images of identifiable individuals constitutes as processing personal information and therefore will be handled in line with this policy and the CCTV Policy.

23.2 The Trust/school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

23.3 If the Trust/school wishes to use images/video footage of pupils in a publication, such as the website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

23.4 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the data protection policy.

DATA RETENTION

24.1 Data will not be kept for longer than is necessary.

24.2 Unrequired data will be deleted as soon as practicable.

24.3 Some educational records relating to former pupils or employees of the Trust/school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Schools must seek guidance from the DPO for these circumstances.

24.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS DATA

25.1 All data provided by the Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this includes electronic communication.

25.2 Data provided by the DBS will never be duplicated.

25.3 Any third parties e.g. audit who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

BIOMETRIC RECOGNITION SYSTEMS

26.1 Where pupil's biometric data is used as part of an automated biometric recognition system (for e.g. pupils use fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedom Act 2012.

26.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Consent

forms part of the Data Collection sheet Appendix B of the Social Media and Photography Policy.

26.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils.

26.7 Parents/carers and pupils can withdraw consent, at any time. The school will make sure that any relevant data already captured is deleted.

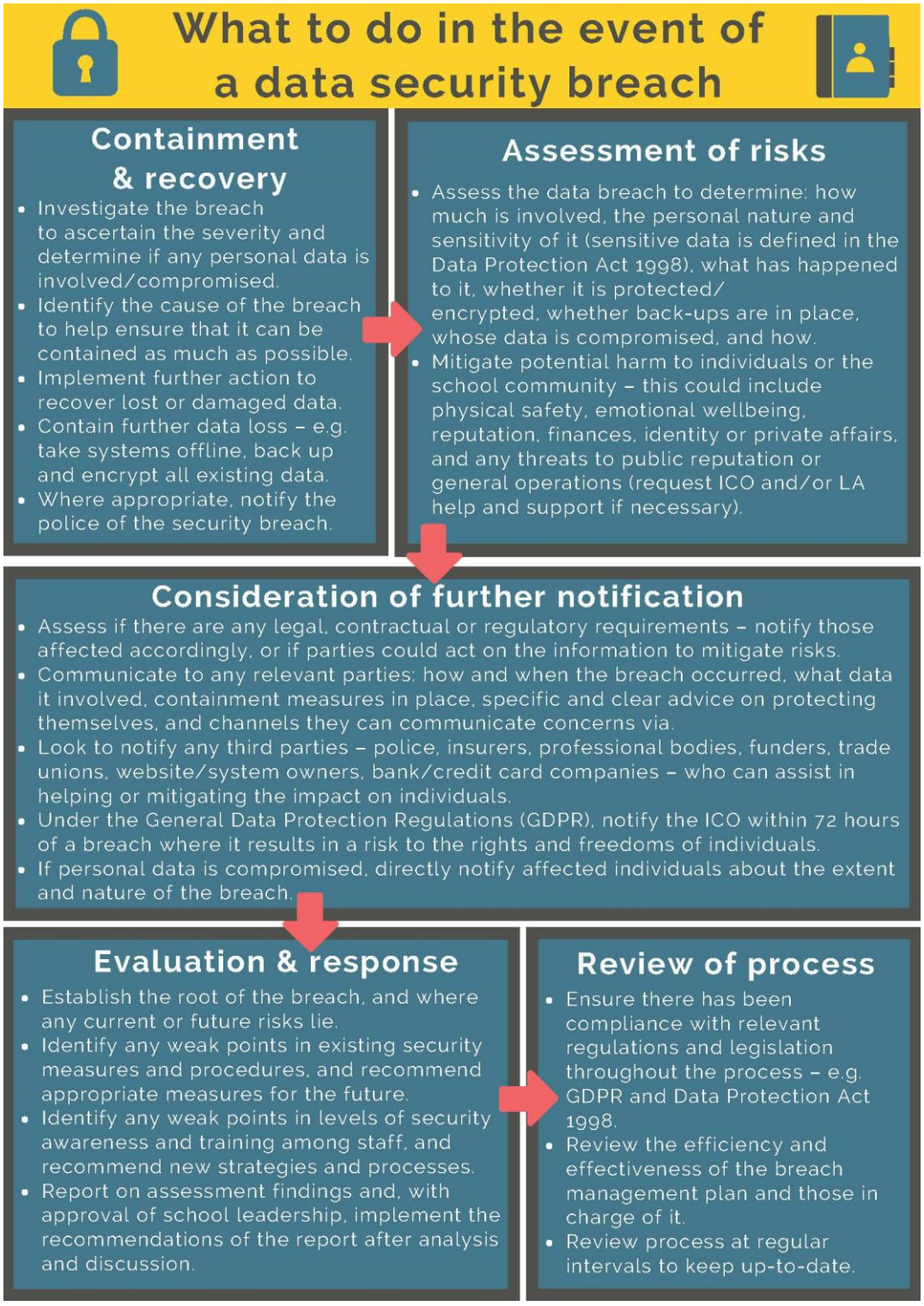
26.8 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, data will not be processed irrespective of any consent given by the pupil's parent(s)/carer(s).

26.9 Where staff members or other adults use the school's biometric system(s), consent will be obtained before activation, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

APPENDIX A: WHAT TO DO IN THE EVENT OF A DATA SECURITY BREACH

Breach or possible breach: DPO to be notified and then the following procedures to be actioned

DPO Contact Details:
Mr Kieran Saul dpo@bridgeacademytrust.org



APPENDIX B: INFORMATION SECURITY

Information security is about what you and Bridge Academy Trust (BAT) should be doing to make sure that personal data is kept safe. This is the most important area of data protection. Most data protection fines have been issued because of information security breaches.

Bridge Academy Trust operates multiple primary and secondary schools in the Essex area. BAT is ultimately responsible for how you handle personal information. In this appendix, the term "Trust" means both Bridge Academy Trust and its schools.

This appendix should be read alongside the following policies relevant to data protection:

- BAT privacy notices for staff, pupils and parents
- Data Protection Policy
- Email Policy
- Acceptable Usage Agreement for staff

This appendix applies to all staff including Members, Trustees, Governors, agency staff, contractors, work experience students and volunteers, who handle personal data. For more information on what personal data is, please see the Data Breaches section above.

Any questions or concerns about your obligations under this appendix should be referred to the Data Protection Officer (DPO).

From this point on, reference to the DPO will be interchangeable with the Headteacher, who will be tasked with forwarding questions or concerns. Questions and concerns about technical support or assistance using BAT IT Systems should be referred to the BAT IT Team or your school's IT Team.

AWARENESS

Information security breaches can happen in a number of different ways. Example of breaches which have been reported in the news include:

- An unencrypted laptop stolen after left on a train
- Personal data taken after a website was hacked
- Sending a confidential email to the wrong recipient
- Leaving confidential documents containing personal data on a doorstep

Please think about what problems what might arise in your team and/or department and what you can do to manage the risks. Speak to your manager and the DPO about improving practices in your team.

All security incidents, breaches and weaknesses should be reported to your school's Data Lead or the DPO. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unblocked at weekends).

The Headteacher, DPO and IT must be informed if you become aware of anything which might mean that there has been a data protection or security breach. This could be anything which puts Personal Data at risk, for example, if Personal Data has been or is at risk of being destroyed, altered,

disclosed, or accessed without authorization, lost or stolen. The DPO must be given all the information you have. This can be completed using the 'Reporting a Data Breach' online form on the trust's GDPR SharePoint site or by speaking to the DPO directly via dpo@bridgeacademytrust.org. If you cannot contact the DPO, or it is outside of school hours, please use the 'Reporting a Data Breach' online form on SharePoint. All of the following are examples of a security breach:

- You accidently send an email to the wrong recipient.
- You cannot find some papers which contain personal data
- Any device (such as a laptop or smartphone) used to access or store personal data has been lost or stolen or you suspect that the security of a device has been compromised.

There are situations where the Trust must report an information security incident to the Information Commissioner's Office and let that information has been compromised know within strict timescales. This is another reason why it is vital that you report information security incidents and data breaches immediately.

DAY TO DAY PRIVACY

Employees should think about data protection and privacy whenever handling personal data. If there are any suggestions for how the Trust could improve its data protection/information security practices or protection individuals' privacy more robustly, please speak to the DPO.

In some situations, the Trust will be required to carry out an assessment of the privacy implications of using personal data in certain ways. For example, when new technology is introduced, where the processing results in a particular risk to an individual's privacy.

These assessments should help the Trust to identify the measures needed to prevent information security incidents from taking place. If you think that if a Data Protection Impact Assessment (DPIA) please speak to your school's data lead or DPO.

SENSITIVE PERSONAL DATA

Data protection is about protecting information about individuals. Something as simple as a person's name or their hobbies could count as personal data. However, some personal data is so sensitive that extra vigilance is needed. This is called Special Category Data (Sensitive). Sensitive personal data is:

- Information concerning child protection matters
- Information about serious or confidential medical conditions and information about special educational needs
- Information concerning serious allegations made against an individual (whether or not the allegation amounts to criminal offence and whether or not the allegation has been proved)
- Financial information (for example about parents and staff)
- Information about an individual's racial or ethnic origin
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition

- Genetic information
- Sexual life or sexual orientation
- Information relating to actual or alleged criminal activity
- Biometric information (e.g. fingerprints used for cashless catering)

Minimizing the amount of personal data held
Restricting the amount of personal data held is needed to keep personal data safe. Employees should never delete personal data unless allowed to do so. For further guidance on when to delete certain types of information, please refer to the Records Management Policy or speak to your school's Data Lead or the DPO.

USING COMPUTERS AND IT

A lot of information security incidents and data protection breaches happen as a result of basic mistakes being made when using BAT IT systems. Here are some tips on how to avoid common problems:

Lock computer screens
Computer screens should be locked when not in use, even if away from the computer for a short period of time.

To lock your computer screen, press the "Windows" key followed by the "L" key. If you are not sure how to do this, then speak to your school's IT Team. Trust computers are configured to automatically lock if not used for a certain amount of time.

Be familiar with Trust IT
Employees should familiarise themselves with any software or hardware used. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

- Make sure you know how to properly use any security features contained in Trust software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this software correctly that the recipient of the document cannot "undo" the redactions.
- You need to be extra careful where you store information containing sensitive personal data. For example, safeguarding information should not be saved on a network drive accessible to all staff. If in doubt, speak to the DPO.

Hardware and software not provided by the Trust
Employees must not use, download, or install any software, or use a service without permission from the BAT IT Team. Employees must not connect (whether physically or by using another method) any device or hardware to BAT IT Systems without permission.

Personal Private Cloud Storage
Employees must not use personal private cloud storage for file sharing accounts to store or share BAT documents, BAT issued cloud storage should only be used.

Portable media devices

The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not permitted unless permission has been given from the DPO, this is reviewed on a case-by-case basis. Any portable media devices authorized to be used must be encrypted.

BAT IT Equipment
Any IT equipment issued by the Trust (this includes laptops, phones, tablets) must be recorded on the Trust IT equipment asset register. Trust IT equipment must always returned to the IT Team even if you think that it is broken and no longer work and the asset register will be updated accordingly.

Passwords
Passwords should be long and difficult to guess. The 'Three random words' approach must be used when setting your password. Words that are memorable to you can be used but avoidance should be given to those which might be easy to guess such as "onetwothree" or are closely related to you personally, such as the names of family members or pets. Further guidance can be found on the National Cyber Security Centre (NCSC) website: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Passwords must not be shared with anyone. Passwords are to be kept secure and confidential. Passwords should not be written down.

EMAILS AND FAXES

When sending emails or faxes employees must take care to make sure that the recipients are correct.

If the email or fax contains sensitive personal data, another member of staff should be asked to double check that the email address/fax number are correct before sending the document.

If a fax contains sensitive data, employees must make sure that the intended recipient is standing by the fax machine to receive the fax.

Encryption
External emails containing sensitive personal data should be encrypted. For example, Word documents can be attached to the email and encrypted with a password which then be forwarded separately to the recipient. You can also type 'encrypt' into the subject line to encrypt the whole email. Internal emails (sent in the trust to another staff member), are encrypted automatically.

Private Email Addresses
Private email address must not be used for BAT related work. Only Trust issued email address should be used. Please note that this rule applies to Trustees, Members and Governors.

PAPER FILES

Keep under lock and key
Employees must ensure that papers which contain sensitive personal data are kept under lock and key in a secure location and that they are never left unattended on desks. Any keys must be kept safe.

Disposal
Paper records containing sensitive personal data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal data should never be placed in the general waste. Paper records must be disposed of in line with the Records Management Policy.

Printing
When printing documents, make sure that you collect everything from the printer straight away, otherwise that there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains personal data, then you must hand it in to your school's data lead.

Put papers away
You should always keep a tidy desk and put papers away when they are no longer needed.

Post

You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something confidential, arrange for it to be sent by courier with tracked and signed for delivery. Consider asking your school's IT team to put the documents on an encrypted memory stick.

Working Off Site (.e.g. school trips or working from home)

The trust recognizes that staff need to take personal data off site for various reasons. This does not breach data protection law if the appropriate safeguards are in place to protect the data.

For school trips, the trip organizer should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that personal data taken off site is returned.

If you are allowed to work from home, then check with your Line Manager what additional arrangements are in place. This might involve working in your trust issued OneDrive account and trust SharePoint sites.

Take the minimum with you
When working away from your school minimum amounts of information should be taken with you. For example, a teacher organizing a field trip might need to take with him/her information about a pupil medical condition. If only ten of twenty pupils are attending the trip, then the teacher should only take information about the ten pupils.

Working on the move
Employees must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing).

Paper records
If you hard copies (i.e. paper records) are needed, they must be kept secure. For example:

- Documents should be kept in a locked case. They should also be kept somewhere secure in additional to being kept in a locked case if left unattended.
- If traveling by train you must keep the documents with you at all times and they should not be stored in luggage racks.
- If travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped.
- If you have the choice between leaving the documents in a vehicle and taking them with you (e.g to the meeting) then you should take them with you and keep them on your person in a

locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plan sight. The risks of this situation should be reduced by only having the minimum of personal data with you.

Public Wi-Fi
Public Wi-Fi must not be used to connect to the internet. For example, if you are working in a café employees will either need to work offline or use 3G/4G or 5G.

Any personal data should not be taken off site in paper format, unless for specified situations where this necessary.

USING PERSONAL DEVICES FOR WORK

Personal devices may be used to complete work. Before using your own device for work, please speak to your school's IT team so that they configure any software.

Appropriate Security Measures should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

Default passwords
If personal devices are used for work which comes with a default password then this password should be changed immediately. Please see section 7 for advice on passwords.

Sending or saving documents to your personal devices
Documents containing personal data (including photos and videos) should not be sent or saved to personal devices unless using your Trust issued OneDrive account. Anything you save to your computer, tablet or mobile phone will not be protected by BAT's security systems.

Friends and family
Employees must take steps to ensure that others who use your devices cannot access anything school related on your device.