THE BRADFIELD GROUP

Data Protection Policy

DOCUMENT INFORMATION

Published to	Internal
Classification	Internal
Reference	Bradfield DP Policy 2023
Owner	The Chief Operating Officer

VERSION HISTORY

Version	Description	Author	Date
0.1	Modifications in red – Draft Policy for discussion	Stuart Williams	April 2020
0.2	Draft Policy for Discussion by DP Committee	Stuart Williams & Andrew Culshaw	April 2020
1.0	Approved by DP Committee		June 2020
1.0	Approved by Audit and Risk Committee		
1.1	Renamed as Group policy	Ashlyn Bingham	June 2022
1.2	Deletion of EU transitional period, change of Compliance Consultant title, definition of Group	Andrew Culshaw	Sept 2023

TABLE OF CONTENT

1. Background

This policy governs the use of Personal Data within the Bradfield Group ("the Group" which comprises St Andrews School Berkshire and Bradfield College). It lays down the principles for the processing of all personal information held by the Group, whether relating to trustees, staff, pupils, parents, volunteers, contractors, suppliers, guests, customers or others.

"Personal Data" means any information relating to a living, natural person, who can be identified either directly or indirectly.

Processing Personal Data includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.

The Group's Data Manager is the Chief Operating Officer and the contact email is gdpr@bradfieldcollege.org.uk.

2. Law and Regulation

The General Data Protection Regulation ("GDPR") 2016 has replaced the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that Personal Data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The GDPR and UK Data Protection Act 2018 ("DPA 2018") apply to the processing of Personal Data wholly or partly by automated means (i.e. by computer), and to the processing, other than by automated means, of Personal Data (i.e. paper records) that form part of a filing system, or are intended to form part of a filing system, in the UK. In addition, the GDPR has a specific territorial scope and will apply to all controllers that are established in the EU (European Union) who process the Personal Data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process Personal Data, in order to offer goods and services to, or monitor the behaviour of data subjects who are resident in the EU.

Defined terms in this policy have the meaning given to them in the GDPR. For ease of reference, definitions and useful terms deriving from the GDPR are set out in the Appendix.

3. Policy and application

3.1. The Bradfield Group's overall compliance with the GDPR is described by this policy and other relevant policies such as IT Security Policy, along with the connected standards and procedures.

3.2. The GDPR and this policy apply to all of the Group's Personal Data processing functions, including those performed on employees', pupils', parents', clients' and suppliers' Personal Data, and any other Personal Data the organisation processes from any source.

3.3. The policy is applicable to the trustees, employees, volunteers and contractors of the Group, regardless of their location. Staff are required to read this policy, familiarise themselves with it and ensure compliance on an ongoing basis.

3.4. Any third parties working with or for the Group, and who have, or may have access to, or process, Personal Data, will be expected to have read and understood, and to comply with this policy.

4. Data Protection Principles

4.1. The Bradfield Group is a data controller and a data processor under the GDPR. All processing of Personal Data must be conducted in accordance with the data protection principles as set out in the GDPR.

4.2. In accordance with Article 5 of the GDPR, the Bradfield Group shall:

4.2.1. process Personal Data lawfully, fairly and transparently;

4.2.2. only obtain Personal Data for specified, explicit and legitimate purposes;

4.2.3. only collect data on a subject that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.2.4. not process or store Personal Data longer that is necessary for processing;

4.2.5. ensure that Personal Data is accurate and kept up to date, with every effort to erase or rectify without delay;

4.2.6. ensure the security of Personal Data, including protection against unlawful processing or accidental loss, destruction, damage or alteration;

4.2.7. demonstrate compliance with the other principles of GDPR (accountability).

5. Data Subjects' rights

5.1. Data subjects have a number of rights regarding their data; these include a right to:

5.1.1. access the Personal Data held on them (to make a subject access request) and know the purposes for which it is processed;

5.1.2. have electronically stored Personal Data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;

5.1.3. know the recipients of the Personal Data processed and the source of the data;

5.1.4. know about any automated decision-making or profiling which makes use of their Personal Data and to object to any automated profiling that is occurring without consent;

5.1.5. not have significant decisions, that will affect them, taken solely by automated process;

5.1.6. request rectification or erasure of Personal Data (the "right to be forgotten")

5.1.7. request the restriction of processing of Personal Data

5.1.8. preventing processing that is likely to cause damage or distress, or processing for direct marketing;

5.1.9. to sue for compensation if they suffer damage by any contravention of the GDPR;

5.1.10. to request the supervisory authority to assess whether any provision of the GDPR has been contravened;

5.2. The Group will ensure that its response to the data access request complies with the requirements of the GDPR.

5.2.1. The Bradfield Group shall respond to any data access request within one month of receipt of the request. When evidently necessary, this period may be extended by no more than two further months (and then only after the Data Subject has been informed of the necessity, within the initial one-month period allowed for a data access response). No charge shall be made for response to any data access request.

5.2.2. Children have an automatic right to access their Personal Data once they are sixteen but may be entitled to access at an earlier age where they evidently possess an informed understanding the issue. Parents have no automatic right to access Personal Data about their child once the child's own entitlement is established.

5.3 Data subjects have the right to make a complaint to the Bradfield Group related to:

5.3.1 the processing of their Personal Data;

5.3.2 the handling of a request from a data subject;

5.3.3 appeals from a data subject on how complaints have been handled

5.4 Complaints should be directed to the Data Manager in the first instance.

6. Lawful Basis for Processing

6.1. The lawful basis of Personal Data Processing must be documented by all Departments and approved by the Data Protection Committee

6.2. In accordance with Article 6 of the GDPR, the Bradfield Group may process Personal Data on the basis of:

6.2.1. **Consent** by the data subject (that is unambiguous, informed, specific, freely given and explicit);

6.2.2. **Contractual necessity**;

6.2.3. Compliance with the Group's **legal obligations**;

6.2.4. **Legitimate interest** of the Group or a third party (except where these are overridden by the rights and freedoms of the data subject);

6.2.5. **Vital Interest** of the data subject;

6.2.6. **Public Interest**;

6.3 Processing of Personal Data on the basis of consent given by the data subject will cease if the data subject withdraws that consent. Furthermore, where processing of Personal Data is on the basis of parental consent, the pupil will have the power to withdraw that consent once they are sixteen and may be entitled to withdraw it at an earlier age where they evidently possess an informed understanding of the issue.

7. Collection of data.

7.1. The Bradfield Group's Privacy Notice requirements are set out in Article 13 of the GDPR. The Groups Privacy Notices will be recorded in the Privacy Notice Register and most are posted on the School and College websites.

7.2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, will include reference to a Privacy Notice posted on the website or link to a Privacy Notice. Privacy Notices will be approved by the Group's DPA.

7.3. The Data Protection Steering Committee and the Department Heads are responsible for ensuring that the Group does not collect information that is not strictly necessary for the purposes set out in the Privacy Notices posted on the School and College websites. The Group will carry out a risk assessment taking into account all the circumstances of the Bradfield Group's controlling or processing operations.

7.4. Department Heads are responsible for ensuring that appropriate policies, standards and procedures are in place to keep Personal Data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

7.5. On at least an annual basis, the Data Protection Steering Committee, with the Department Heads, shall review the retention dates of all Personal Data processed by the Group, by reference to the data inventory, and will identify any data that is no longer required in the context of the purpose specified in the pertinent Privacy Notice. This redundant data will be securely deleted/disposed.

7.6. The Data Protection Steering Committee shall review, at least once a year, all data collection methods to determine that collected data continues to be adequate, relevant and not excessive.

8. Security of data

8.1. All trustees, employees and volunteers are responsible for ensuring that any Personal Data that the Group processes and for which it is responsible, is protected against accidental, unauthorised or unlawful loss or damage, and against unauthorised access, use, modification or disclosure.

8.2. All Personal Data will be accessible only to those who are authorised and need to use it. Access will only be granted in line with the IT Security Policy.

8.3. All Personal Data will be treated with the highest security and will be kept:

8.3.1. in a lockable room with controlled access; and/or

8.3.2. in a locked drawer or filing cabinet; and/or

8.3.3. (if computerised) encrypted or password protected, in line with the requirements of the IT Security Policy; and/or

8.3.4. stored on (removable) computer media which are encrypted in line with IT Security Policy.

8.4. The Bradfield Group shall control and monitor the use of locally installed applications, Cloud Services and Third-party cloud applications' permissions to Cloud services, which process or can process Personal Data. Only those applications will be used that provide adequate protection of Personal Data.

8.5. Processing of Personal Data 'off-site' and away from the Group's offices presents a potentially greater risk of loss, theft or damage to Personal Data. Staff will process Personal Data off-site only if specifically authorised by the relevant Department Head to do so.

8.6. Personal Data shall be disposed in a manner that ensures it cannot be recovered or reconstructed. Manual records shall be directly shredded or disposed to a "secure, confidential" bin to await professional shredding. Hard drives of redundant computers will be securely wiped (zeroed), defected drives will be removed and destroyed (if they have not been encrypted).

8.7. In determining appropriate technical and organisational measures to ensure the security of any Personal Data, the Data Protection Committee will consider: the extent of possible damage or loss that might be caused to individuals (e.g. staff, pupils or parents) if a security breach occurs; the effect of any security breach on the Bradfield Group itself; any likely reputational damage, including the possible loss of trust.

9. Disclosure of data

9.1. The Group will ensure that Personal Data is not disclosed without appropriate authorisation to third parties (including family members, friends, government bodies, the Police or Auditors.)

9.2. All employees will exercise caution when asked to disclose to a third-party Personal Data held on another individual. As a general rule, disclosure to a third party will be possible: with the consent of the data subject; in fulfilment of a contract; in pursuit of the legitimate interests of the School and / or College, to comply with legal obligations; to protect the vital interests of the data subject; in the public interest.

9.3. Employees will seek guidance before any disclosure which is not explicitly, specifically and unambiguously authorised by the data subject.

10. Retention and disposal of data

10.1. The Group will not keep Personal Data in a form that permits identification of data subjects for any period which is longer than necessary, in relation to the purpose(s) for which the data was originally collected.

10.2. The retention period for each category of Personal Data is set out in the School and College's Information and Records Retention Policies.

10.3. The Data Protection Steering Committee must specifically approve any data retention that exceeds the retention periods defined in Information and Records Retention Policy, and will ensure that the justification for extended retention is clearly identified and in line with the requirements of the data protection legislation. This formal approval and its justification will be a matter of written record.

10.4. Where Personal Data is retained beyond the processing date, it will be minimised and encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

11. Data transfers outside of the EEA

11.1. The transfer of Personal Data outside of the EEA is **prohibited** unless one or more of the specified safeguards, or exceptions, apply:

11.1.1. An adequacy decision;

11.1.2. US Privacy Shield;

11.1.3. Model contract clauses;

11.1.4. Corporate Binding Rules;

11.1.5. Exceptions, as defined in the GDPR

11.2. In all cases, if the Bradfield Group intends to transfer data outside the EEA it will first seek guidance and approval from the Compliance Consultant.

11.3. Prior to introducing any new Cloud Services or a new application within the existing Cloud Service, St Andrew's School and / or Bradfield College will first seek guidance and approval from the Compliance Consultant.

12. Information asset register/data inventory

12.1. The Bradfield Group will establish and maintain a data inventory and data flow process to comply with GDPR Article 30 requirements.

12.2. Procedures for informing the Group on risks associated with the processing of particular types of Personal Data shall include:

12.2.1. assessing the level of risk to individuals associated with the processing of their Personal Data, including data protection impact assessments (DPIAs) which are carried out in relation to the processing of Personal Data by St Andrew's School and / or Bradfield College, and in relation to processing undertaken by other organisations on behalf of the Group;

12.2.2. managing any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with GDPR and this policy;

12.2.3. carrying out a DPIA of the impact of the envisaged processing operations on the protection of Personal Data, particularly where the type of processing involves the use of new technologies which may result in a high risk to the rights and freedoms of Data Subjects;

12.2.4. escalation to the Data Protection Steering Committee where, as a result of a DPIA, it is clear that the Group is about to commence processing of Personal Data that could cause damage and/or distress to the data subjects;

12.2.5. escalation to the Information Commissioner's Office where the Compliance Consultant expresses significant concerns, either as to the potential damage or distress, or the quantity of data concerned.

13. Roles and Responsibilities under GDPR

13.1. The Bradfield Group Council and all those in managerial or supervisory roles throughout the Group are responsible for developing and encouraging good information handling practices within the School and College; responsibilities are set out in individual job descriptions.

13.2. The Data Protection Committee (comprised of the COO and his PA, the Director of IT, the Procurement Manager, the Compliance Consultant and the GDPR Consultant, is accountable to the Bradfield Group Council for the management of Personal Data within the Group.

13.3. The Compliance Consultant reports to the COO and is accountable to the Bradfield Group Council for monitoring compliance with data protection legislation and acknowledged good practice.

13.4. Compliance with data protection legislation is the responsibility of all Employees/Contractors of the Bradfield Group.

13.5. Employees/Contractors of the Bradfield Group are responsible for ensuring that any Personal Data about them and supplied by them to the Bradfield Group is accurate and up-to-date.

14. Policy Compliance

14.1. **Compliance Measurement:** The Compliance Consultant will assess compliance to this policy through various methods.

14.2. **Exceptions:** Any exception to the policy will be approved by the Data Protection Steering Committee in advance.

14.3. **Non-Compliance:** Any breach of this policy and/or GDPR may result in disciplinary action or termination of contract, may be reported to the "ICO" and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Appendix

Client Personal Data - any Personal Data Processed by St Andrew's School and / or Bradfield College or the Bradfield Group's Sub processor on behalf of the Client pursuant to or in connection with the Master Service Agreement.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal Data – 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.

Special categories of Personal Data – Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of Personal Data held by an organisation.

Processing – any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. There is an obligation on the controller to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data.

Filing system – any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.