POLICY STATEMENT

Policy	Data Protection policy
School Department	Administration

Date Written	1 September 2019
Written by	Compliance Officer
Approved by	SMT
Date of Approval	11 September 2019
Next major review date	1 September 2021
Location and disseminations	A copy of the policy can be found in the school admin office.

DATA PROTECTION POLICY

Our Commitment:

Buckswood School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the General Data Protection Regulation (GDPR).

1. Interpretation

1.1 Definitions: In this document the following terms shall have the following meanings:

School: Buckswood School Ltd

School Personnel: all employees, workers contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our School Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity.

Data Protection Manager (DPM): the person (or team of persons) with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data. Personal data can be factual, e.g. a date of birth, or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the School collects information about them.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording, holding, amending, retrieving, using, disclosing, erasing or destroying data or transferring it to third parties.

Related Policies: the School's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. Introduction

This Policy sets out how Buckswood School Ltd ("we", "our", "us", "the School") handle the Personal Data of our customers, suppliers, workers, contractors and other third parties.

It applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all School Personnel ("you", "your"). You must read, understand and comply with it when Processing Personal Data on our behalf and attend training on it if required. This Policy sets out what we expect from you in order for the School to comply with applicable law. It is intended to help School Personnel work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data. Your compliance with this Policy is mandatory and any breach of it may result in disciplinary action.

This Policy is an internal document and should not be shared with third parties without prior authorisation from the DPM.

This Policy does not set terms or conditions of employment or form part of your employment contract.

3. Scope

The correct and lawful treatment of Personal Data helps to maintain confidence in the School and will promote the success of the business and its operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The School is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All departments are responsible for ensuring that School Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to achieve this.

The DPM is responsible for overseeing this Policy.

Please contact the DPM with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being followed. In particular, you must always contact the DPM in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (see section 5.1 below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see section 5.2 below);

(c) if you are unsure about the retention period for the Personal Data being Processed (see section 9 below);

(d) if you are unsure about what security or other measures you need to implement to protect Personal Data (see section 10.1 below);

(e) if there has been a Personal Data Breach (section10.2 below);

(f) if you need any assistance dealing with any rights invoked by a Data Subject (see section 12);

(g) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see section 13.3 below) or plan to use Personal Data for purposes other than what it was collected for;

(h) If you need help complying with applicable law when carrying out direct marketing activities (see section 13.4 below); or

(i) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see section 13.5 below).

4. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations.;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

5.2 Consent

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is

given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Explicit Consent is required for Processing Sensitive Personal Data unless we can rely on another legal basis of Processing. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the School can demonstrate compliance with Consent requirements.

5.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide specific information to Data Subjects when collecting Personal Data. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and written in clear and plain language. Where relevant the Privacy Notices should be written in a form understandable by children.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR when the Data Subject provides the Personal Data. The School does this by means Privacy Notices, copies of which are available on its website.

Our pupil privacy notice can be found at:

https://www.buckswood.co.uk/wp-content/uploads/2017/03/Privacy-Notice-Pupils.pdf

Our staff privacy notice can be found at:

https://www.buckswood.co.uk/wp-content/uploads/2017/03/Privacy-Notice-Employees.pdf

When Personal Data is collected indirectly (for example, from a third party or publically available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6. Purpose limitation

Personal Data must be collected only for specified and legitimate purposes and must not be further Processed in any manner incompatible with those purposes.

We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

7. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You must not Process Personal Data for any reason unrelated to your job duties. You may only collect Personal Data that you require for your job duties: do not collect excessive or irrelevant data.

We must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with any data retention guidelines or policy issued by the School from time to time.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the purposes for which we originally collected it.

The School will maintain retention guidelines to ensure that Personal Data is deleted after the period for which it needs to be kept has expired. You must comply with the School's guidelines on data retention. You are required to take all reasonable steps to destroy or erase all Personal Data that we no longer require in accordance with the applicable retention guidelines. This may include requiring third parties to delete such data where relevant.

We must also ensure that Data Subjects are informed of the period for which data is stored in any applicable Privacy Notice.

10. Security integrity and confidentiality

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

We will develop, implement and maintain appropriate safeguards and regularly evaluate and test the effectiveness of those safeguards to ensure the security of our Processing of Personal Data. You have a personal responsibility for protecting the Personal Data we hold and must adhere to our security measures and guard against the unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

Hard copy data, records, and personal information must stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school nurse.

Sensitive or personal information and data should not be removed from the School site, however the School acknowledges that some staff may need to transport data between the School and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on School visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be taken on an encrypted work computer
- Personal Data may not be transferred by USB device

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR to protect Personal Data.

10.2 Data Disposal:

The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: *https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf*

The school has identified a qualified source for disposal of IT assets and collections. The school also uses Shred-it to dispose of sensitive data that is no longer required.

10.3 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You should immediately contact the DPM, follow any instructions given and preserve all evidence relating to the potential Personal Data Breach.

11. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. This limitation is unlikely to impact on the School's operations. However, please note that you may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPM;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between the School and the Data Subject.

12. Data Subject's rights and requests

Data Subjects have rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(i) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(j) make a complaint to the supervisory authority; and

(k) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your line manager or the DPM and comply with the School's Data Subject response process.

13. Accountability

13.1 As the Data Controller the School is responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and document GDPR compliance including:

(a) undertaking audits and reviews of Processing activities;

(b) appointing an executive as accountable for data privacy;

(c) implementing policies and guidelines;

(d) providing training; and

(e) keeping records of Processing.

13.2 Record keeping

The GDPR requires us to keep appropriate records of data Processing activities including, by way of illustration descriptions of Personal Data types, Data Subject types, Data Subjects' Consents and procedures for obtaining Consents where applicable, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, retention periods and security measures

13.3 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

In particular we aim to assess what Privacy by Design measures can be implemented on our programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks posed by the Processing.

The School must also conduct DPIAs in respect to high risk Processing such as when implementing major system or business change programs involving the Processing of Personal Data.

A DPIA must include:

(e) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(f) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(g) an assessment of the risk to individuals;

(h) the risk mitigation measures in place; and

(i) demonstration of compliance.

13.4 Direct marketing

Like all businesses, the School is subject to certain rules and privacy laws when marketing to its customers.

A Data Subject's prior consent is required for electronic direct marketing (for example by email). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression

involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.5 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the School if the recipient has a job-related need to know the information.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- Other schools
  If a pupil transfers from Buckswood School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the

next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- Examination authorities
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- Health authorities
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- Police and courts
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- Social workers and support agencies
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- Educational division
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given in the Privacy Notices. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them by amending the Privacy Notice and drawing this to their attention.

With regard to data subject access requests the School will not generally be required to disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition

- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil or the School in an examination script
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- with regard to a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

and School personnel should seek advice from the DPM with regard to any data subject access request before responding.

14. Changes to this Privacy Standard

We reserve the right to change this Policy at any time and will publish details of any changes when made.

I confirm that I have read and understood the contents of this policy:

Signed

Employee Name

Date