Personal Data Policy
January 2021

Introduction

Baytree School will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature (BECTA – Good Practice in information handling in schools – keeping data secure, safe and legal – September 2008).
It is the responsibility of all members of Baytree school community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

Have permission to access that data
Need to have access to that data

Any loss of personal data can have serious effects for individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution. All transfer of data is subject to risk of loss or contamination.
Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (2018) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow.
It:

- Provides clarity on the definitions used in the GDPR in the UK context.
- Ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained.
- Provides appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Sets the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

Policy Statements

Baytree School will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.
Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the 'Fair Processing Code' and lawfully processed in accordance with the 'Conditions for Processing'.

Personal Data

Baytree school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

> Personal information about members of the school community, including pupils, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship/contact details, health records, disciplinary records

Curricular/academic data e.g. class lists, pupil progress records, reports, references

Professional records e.g. employment history, taxation and national insurance records, appraisal records and references

Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

Responsibilities
Baytree School's Senior Information Risk Officer (SIRO), PA to the Headteacher, will keep up to date with current legislation and guidance and will:

Determine and take responsibility for the school's information risk policy and risk assessment

Appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil information, staff information/assessment data etc). The IAOs will manage and address risks to the information and will understand

What information is held and for what purpose
How information has been amended or added to over time
Who has access to protected data and why

Everyone in Baytree has the responsibility of handling protected or sensitive data in a safe and secure manner.
Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.
Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration
Baytree School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – the 'Privacy Notice'
Under the 'Fair Processing' requirements in the Data Protection Act, the school will inform parents/carers of all pupils/students of the data they hold on the pupils/students, the purposes for which the data is held and the third parties (e.g. LA, Gov.uk, DfE, etc) to whom it may be passed. This privacy notice is passed to parents/carers and is available on the school's website. Parents/carers of young people who are new to the school will be provided with the Privacy Notice on joining the school.

Training and Awareness
All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

Induction training for new staff
Staff meetings/briefings/Inset
Day to day support and guidance from Information Asset Owners
Online training updated annually at the beginning of the school year by all staff and Governors.

Identification of Data
The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

Secure Storage of and access to Data
Baytree School will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
All users will be given secure usernames and strong passwords which must be changed regularly. Usernames and passwords must never be shared.
Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used. When personal data is stored on any portable computer system, USB stick or any other removable media:

The data must be encrypted and password protected.
The device must be password protected.
The device must offer school approved virus and malware checking software.
The data must be securely deleted from the device, in line with school policy ~~(below)~~ once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

All paper based material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data.

Secure transfer of data and access out of school
Baytree School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

Users may not remove or copy sensitive or personal data from the school, or transfer between premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school (all staff sign an acceptable use contract at the beginning of each school year).
When data is required by an authorised user from outside the school premises (for example, a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform through the VPN.

Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of Data
Baytree School will comply with the requirements for the safe destruction of personal data when it is no longer required.
The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with Government guidance, and other media must be shredded, incinerated or otherwise disintegrated.

Audit Logging/Reporting/Incident Handling
As required by the 'Data Handling Procedures in Government' document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the SLT.
The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an Acceptable Use Policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

Baytree School has a policy for reporting, managing and recovering from information risk incidents, which establishes

A 'responsible person' for each incident
A communications plan, including escalation procedures
which results in a plan of action for rapid resolution and
A plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.
All incidents are also raised within the process/procedures of the E-Safety Policy.

For further information please refer to:
Data protection policy
Data protection factsheet – 2018
Data protection Act 2018
E-Safety policy
Acceptable use policy
BECTA – Good Practice in information handling in schools – keeping data secure, safe and legal – September 2008

Review of Policy

Reviewed by FGB: 27th January 2021			
Next Review due: January 2022			