Bitterne C of E Primary School

Policy for Data Protection

Headteacher

Last review – September 2022

Next review – September 2023

Chair of Governors- Amanda Humby

PURPOSE

The EU's General Data Protection Regulation (the "**GDPR**"), as well as domestic legislation that remains in place until the GDPR comes into force on 25 May 2018 or that enhances or replaces the GDPR from time to time, lay down rules to protect personal privacy and uphold individuals' rights. The Data Protection Rules apply to anyone who "processes" (e.g. handles or has access to) individuals' personal data. Now that the UK has left the EU, there is a transition period until the end of 2020 to allow time to negotiate a new relationship with the EU. During the transition period the GDPR will continue to apply in the UK. The school will continue to follow existing guidance on the GDPR and monitor the ICO website for any developments in guidance during the remainder of the transition period.

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

SCOPE

This Policy applies to all individuals working in the school. For the purposes of this Policy, the term "**staff**" means all employees within the school, including permanent, fixed-term and temporary staff; as well as governors, third party representatives, agency workers and volunteers.

This policy applies to all personal information however it is collected, used, recorded and stored by the school, and whether it is held on paper or electronically.

DATA PROTECTION PRINCIPLES

The GDPR provides six data protection principles as well as a number of additional duties, which the school will follow to ensure good data handling:

1) **Lawfulness, fairness and transparency**: Personal data shall be processed fairly, lawfully and in a transparent manner;
2) **Purpose limitation:** Personal data shall be obtained only for one or more specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes (unless it is for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes);
3) **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary for its processing purposes;
4) **Accuracy:** Personal data shall be accurate and where necessary kept up to date, and every reasonable step must be taken to ensure that data which is inaccurate is erased or rectified without delay;
5) **Storage limitation:** Personal data shall not be kept in a form which allows the identification of individuals for longer than is necessary for the purpose for which it is processed (unless it is solely for archiving purposes in the public interest, statistical purposes or scientific or historical research purposes and appropriate security measures have been implemented);
   Integrity and confidentiality: Personal data shall be processed in a manner that ensures its security, using appropriate technical and organisational security measures, in order to

protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;

RESPONSIBILITIES

The Data Protection Rules require certain organisations to appoint a Data Protection Officer ("**DPO**") giving them prescribed responsibilities. The Data Protection Officer for the school is the David Scott-Batey (based at Springwell School)

The DPO will have overall responsibility for the school's compliance with the Data Protection Rules. The DPO's responsibilities will include, but are not limited to, the following tasks:

- Keeping up to date with any changes to the way the school processes data;
- Taking steps to promote individuals' awareness of why the school need their personal information, how the school will use it and with whom the school may share it;
- Setting out clear procedures for responding to requests for access to personal information, known as subject access requests;
- Arranging appropriate data protection training for school staff so they are aware of their responsibilities;
- Ensuring that staff are aware of this Policy and are following it; and
- Ensuring that new software or new services for the school are compliant, and that data protection impact assessments are carried out where necessary.

The school will ensure that the DPO is provided with resources and support to fulfil all of their responsibilities. Individuals may contact the DPO regarding any issues relating to the processing of their data by the school. Contact details for the DPO can be found at the end of this Policy, in the Contact Information section.

The school can delegate the day-to-day responsibility for ensuring compliance with the Data Protection Rules and this Policy and appoint a Data Compliance Officer (**DCO**). Although the DPO will have overall responsibility for the compliance of the school with the Data Protection Rules and this Policy, the DCO will be responsible within their school for the following tasks: The Data Compliance Officer for the school is Clare Horan.

- Ensuring that individuals are made aware of the Privacy Notice (see appendices) as and when any information is collected;
- Checking the quality and accuracy of the information held by the school;
- Applying the Southampton City Council's records retention schedule to ensure that information is not held longer than necessary by the school; Please follow this link to view the retention schedules; http://www.southampton.gov.uk/contact-us/privacy-cookies/privacy-policy.aspx#retention
- Ensuring that when information is authorised for disposal, it is done so appropriately;
- Ensuring that appropriate security measures are in place to safeguard personal information, whether it is held in paper files or electronically;
- Ensure staff are aware of the Data Breach Procedure and how to report a data breach;
- Only sharing personal information when it is necessary, legally appropriate to do so and in accordance with the Privacy Notice; and
- Ensuring that staff in the school are aware of this Policy and are following it.

The school will renew its registration with the Information Commissioner's Office (ICO) if and when necessary and pay any fees due to the ICO.

STAFF RESPONSIBILITIES

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely;
- Personal information is not disclosed orally, in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party;
- Information or data about pupils is only shared with other staff as necessary and only by secure methods. Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases; and
- Any additional associated policies are complied with (see section 1).

PRIVACY NOTICES

When any information is collected about individuals, they must be made aware of the Privacy Notices (see Appendix 1 and 2). The Privacy Notice provides information about what, why and how information is processed. You should make yourselves aware of the Privacy Notice, which should be read in line with this Policy.

Processing, Disclosure and Sharing of Information

The school processes personal data for a number of different purposes including:

Lawful Ground for Processing	**Examples**
Where we have your consent	Posting photographs of a pupil on the school's or the school's website. Providing pupil information for the administration of a school trip.
Where it is necessary for the performance of a contract to which an individual is party	Providing information to a school photographer about photos required for a pupil. Providing employment services (such as payroll and references).
Where it is necessary for compliance with a legal obligation	Passing on pupil information to the Department for Education Passing on pupil information to the Local Authority

	Use of personal information to consider staff suitability to work in school. To ensure that staff have the Right to work in the UK.
Where it is necessary to protect the vital interests of an individual	Passing on information about a pupil's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that pupil or another individual.
Where it is necessary for performance of a task in the public interest	Updating and maintaining a pupil's educational record as the pupil develops and progresses Carrying out safeguarding activities

The school, may also share data that they hold with members of staff, relevant parents/guardians, other schools, Local Authorities, the Department for Education, Ofsted, statutory bodies and other authorities where it is necessary to do so or where we are permitted to do so e.g. for the prevention of crime, to health professionals and examination bodies or any other body that the school deems appropriate. Any sharing of data must be in accordance with the Data Protection Rules, this Policy and the Privacy Notice.

If the school receives any enquiries from third parties, particularly by telephone, it is important to be careful about what data is disclosed. The following steps should be followed:

- Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the information they have requested;
- Require the third party to put their request in writing in order to verify their identity and their entitlement to the data requested;
- If in doubt, refer the request to the DCO;
- When providing information to a third party, do so only in accordance with the Data Protection Rules, the Privacy Notice and this Policy; and
- Consider if a parent or guardian should have access to a pupil's information or whether the pupil is old enough to make any requests themselves.

IMAGES

- ***Websites –*** Where personal information, including images, is placed on the school's website, consent will be sought from the individual as appropriate.
- ***Photographs*** – Permission will be sought from the individual by the school before photographs of the individual are used or displayed, including in the school prospectus, newsletter or any other such publication where they can be clearly identified individually.

Requests for Access to Information

Any person, whose personal information is held by the school, has a right to ask for access to this information. These requests will be free-of-charge in almost all circumstances on and after 25 May 2018. Requests must be made in writing to the school's DCO or the school's DPO. A response to any such request must be dealt with within one month from the date on which the request was received. The DCO must ensure that the Headteacher is made aware of any such request.

Unlike the separate right of access to a pupil's progress and attainment record, the right to make a subject access request is the pupil's right. Parents/guardians are only entitled to access information about their child (by making a request) if the child is unable to act on their own behalf e.g. because the child is not mature enough to understand their rights or if the child has given their consent. If you are unsure about whether or not to provide information about a pupil to a parent or guardian, please speak to your DCO or the Trust's DPO before providing any information.

Requests that fall under the Freedom of Information Act 2000 will be dealt with in accordance with Southampton City Council's FOIA policy and procedures.

More information and detailed guidance can be found by visiting www.ico.gov.uk.

Individuals also have other legal rights under the Data Protection Rules, including to object to and prevent processing in certain circumstances and to have inaccurate personal data corrected or deleted. More information on these rights can be found in the Privacy Notice under "Requesting access to personal data".

Complaints and Breach Notification

Complaints should be made following and will be dealt with in accordance with the school's complaint policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner (ICO). www.ico.gov.uk

Information about how the school, will deal with data breaches, including who to contact if they believe there may have been a data breach, can be found in the school's Data Breach Procedure (Appendix 3). The Data Protection Rules contain requirements about handling of breaches, which the school must comply with, so staff must ensure that they report any breaches in accordance with the Data Breach Procedure.

Contact Information

Your first point of contact should be the DCO for your school, Clare Horan – Email Address: info@bitterneceprimary.net Their information should be available in the School Office. If the DCO is unavailable, you should contact the school's DPO.

The Data Protection Registration Number for Bitterne CE Primary School is ZA167877. A copy of the registration can be found at https://ico.org.uk/ESDWebPages/Entry/ZA167877

The school's DPO is David Scott-Batey and can be contacted by email at

dscott-batey@springwellschool.net, by telephone on 023 80445981 or at the following address: School Business Director, Springwell School, Hinkler Road, Thornhill, Southampton, SO19 6DH

1. Associated Policies

- Complaints Procedure
- Acceptable Use of IT Policy

Appendix 1 -Privacy Notice (How we use pupil information)

Why do we collect and use pupil information?

We collect and use pupil information under:

Data Protection Act 1998 (until 25th May 2018)

- Schedule 2(5)(b) - The processing is necessary for the exercise of any functions conferred on any person by or under any enactment
- Schedule 2(5)(d) – The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person
- Schedule 3(7)(b) - The processing is necessary for the exercise of any functions conferred on any person by or under any enactment

General Data Protection Regulation (EU) 2016/679 (from 25th May 2018)

- Article 6(1)(e) – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Article 9(2)(g) – the processing is necessary for reasons of substantial public interest

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Academic progress / assessment data
- Relevant medical information
- Special educational needs information
- Exclusions / behavioural information

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

The local authority will hold pupil data in accordance with its Retention Schedule:
http://www.southampton.gov.uk/contact-us/privacy-cookies/privacy-policy.aspx#retention

The school will hold pupil data as outlined in the LA Retention Schedule.

Who do we share pupil information with?

We routinely share pupil information with:

- Schools / other education providers
- our local authority
- the Department for Education (DfE)
- the NHS
- other local authorities

For further details, please see “Why do we collect and use pupil information?”, above.

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils’ data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We also share pupil information to:

- Meet our statutory duty to create and maintain an admission register under the Education (Pupil Registration) (England) Regulations 2006 and subsequent amendments, without which schools are unable to enrol a pupil.
- Support teaching and learning. In order to facilitate this, we may share information with the software supplier (listed at the end of this document) to set up the systems needed for pupils and parent/carers to access.
- Monitor and report on academic progress.
- Provide appropriate pastoral care (Keeping Children Safe in Education 2016).
- Assess how well we, as an education provider, are doing.
- Co-operate with Southampton City Council and external partners to improve the well-being of children, under the duty of the Children Act 2004. Working Together to Safeguard Children (2015)
- Share information with Southampton City Council and external partners to support the duty to safeguard and promote the welfare of children, under the Children Act 1989, Section 17. Working Together to Safeguard Children (2015)
- Share data with professionals commissioned by the school or working with a pupil such as the School Nurse or health services.
- Comply with our statutory duty under the Education (Pupil Information) (England) Regulations 2005 Statutory Instrument and subsequent amendments in The Education (Pupil Information) (England) (Amendment) 2008 to create a Common Transfer File when a child ceases to be registered at a school and becomes a registered pupil at another school in England or Wales. This would also apply to pupils who are dually registered at more than one school. If a Common Transfer File cannot be sent to a new school when a pupil leaves, one must be sent to the DfE Lost Pupil Database.

- Provide information via statutory census returns to the DfE and in turn this will be available for the use of Southampton City Council to carry out its official functions, or a task in the public interest. Further information can be found online at https://www.gov.uk/government/publications/school-census-2016-to-2017-guide-for-schools-and-las
- Send pupil information to Southampton City Council on a regular basis in accordance with our information sharing agreement to enable the local authority to meet its duty under data protection legislation to ensure that the data it holds is accurate and also to carry out its official functions, or a task, in the public interest.
- Notify Southampton City Council on a termly basis of all pupils on a reduced timetable so that the local authority can comply with statutory Ofsted requests for data at the time of inspection.
- Comply with the statutory requirements of the Education (Pupil Registration) (England) Regulations 2006 and subsequent amendments, notifying Southampton City Council if a child leaves the school and providing forwarding details. A failure to provide this information will result in pupils being record as a "Child Missing Education", in accordance with the government definition.
- Provide attendance information to Southampton City Council so that its duties under the Anti-Social Behaviour Act 2003, Section 444 of the Education Act 1996 and Section 36 of the Children Act 1989 (Education Supervision Orders) can be met.
- Provide exclusion information to Southampton City Council so that its duty Under Section 19 of the Education Act 1996 can be met.
- Meet our duty to provide information about any exclusions within the last 12 months to the Secretary of State and (in the case of maintained schools and PRUs) the local authority, in accordance with The Education (Information About Individual Pupils) (England) Regulations 2006.
- When your child applies for further education or training, the school / LA may forward information to colleges or providers in order to aid your child's transition into further education or training

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our Data Protection Officer,
……...

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:

- Andy Peterson (Headteacher) info@bitterneceprimary.net

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

www.youngsouthampton.org/privacynotice.aspx and
http://media.education.gov.uk/assets/files/doc/w/what%20the%20department%20does%20with%20data%20on%20pupils%20and%20children.doc
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

- If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:
- **Solicitor for Education:** Legal Services, Southampton City Council, Ground Floor, Civic Centre, SO14 7LY
- **Public Communications Unit:** Department for Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
- Website: www.education.gov.uk
- Email: www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288

School postal address	**Bitterne CE Primary School** **Brownlow Avenue** **Southampton** **SO19 7BX**
School e-mail address	info@bitterneceprimary.net
School telephone number	**02380499494**
Software supplier	**Capita – Sims – Pupil Information Management Systems** **School's Cash Office – School Meals /Parents Evening / Extended Day** **CPOMS – Child Related Information** **Libresoft – Library Systems**

	Data Transfer – DFE s2s / SCC Anycomms **Springwell School – IT Support** **Tapestry** **Seesaw** **Pearson Education-Bug Club – online reading** **Time Tables Rock Stars** **Edukey – Provision Mapper – SEND** **Little Wandle**

Appendix 3: Data Breach Procedure

1. About this procedure

This procedure describes the actions that must be taken by staff to report any incident which may result in a personal data breach. A "personal data breach" is defined in Article 4(12) of the General Data Protection Regulation as:

"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."

Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a personal data breach. The term "incident" is used in this policy to describe any situation which may, upon investigation, turn out to be a personal data breach.

This procedure should be read in conjunction with the Data Protection Policy.

2. Identifying an incident

An incident may come to light in a number of ways. For example, it could occur by:

- direct observation e.g. where a member of staff spots that personal data has been sent to the wrong email address;
- being reported to us by a pupil or parent: e.g. where a pupil notifies us that she/he has received personal data relating to another pupil;
- being reported to us by another party, such as a contractor, a local authority or a member of the public; or
- an audit /review revealing that an incident had occurred.
-

3. Actions to take once an incident has been identified

Whenever an incident is identified, the following actions must be taken:

	Action	Responsibility	Timelines
1.	Report the incident to the Data Compliance Officer for the school (or, if unavailable, the Data Protection Officer of the School)	Member of staff who was first made aware of the incident	**Immediately after the incident is identified**
2.	Investigate and identify the full details of the incident to identify the cause	Data Compliance Officer for the school (with the assistance of the colleague who reported the incident)	**As soon as possible following the incident being reported**
3.	Identify any remedial action (see section 4, below)	Data Compliance Officer for the school	**As soon as possible following the incident being reported**
4.	Complete a formal Personal Data Breach Form and return it to the Trust's Data Protection Officer	Data Compliance Officer for the school	**Within 48 hours of the incident being identified**
5.	Review the Personal Data Breach Form and determine whether the incident constitutes a personal data breach or a 'near miss' (i.e. an incident which does not meet the definition of a personal data breach)	Data Protection Officer (in conjunction with the Data Compliance Officer for the school)	**As soon as possible following step 4**
6.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual data subjects, of the personal data breach (see section 5, below)	Data Protection Officer (in conjunction with the Data Compliance Officer for the school)	**As soon as possible following step 4**
7.	If necessary, notify the ICO of the personal data breach	Data Protection Officer	**Within 72 hours of the incident being identified**
8.	If necessary, notify individual data subjects of the personal data breach	Data Protection Officer	**Without undue delay (in practice this should be done as soon as possible)**

4. Taking remedial action

Following the reporting of the issue, the School's Data Protection Officer shall advise the relevant Data Compliance Officer what remedial action must be taken, in particular where pupils or parents are affected in any way by the personal data breach. Pupils or parents may suffer distress and inconvenience where they are aware that a breach has occurred. In some cases, they may be at risk of suffering financial detriment or physical harm as a result of the breach.

Remedial action should seek to mitigate any risks the pupil or parent has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the school's reputation. Action will be dependent on case specifics, but the Data Protection Officer should consider the School's responsibility to act in the best interests of pupils and parents.

Remedial action might include the following:

- If personal data is in the hands of a third party, it should be retrieved from the third party or deleted from the third party's IT system (please speak to IT for assistance);
- If the breach arose as a result of an IT issue, the source of the issue should be identified and rectified (please speak to IT for assistance);
- If the breach arose as a result of human error, the individual should be made aware of the error and where appropriate asked to undertake additional training or (only in the most serious cases) be subjected to disciplinary action.

5. Notifying a personal data breach

Under the General Data Protection Regulation, there is an obligation to report a personal data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of us becoming aware of the breach.

There is an exception to this reporting requirement where the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the School's Data Protection Officer following receipt of the Personal Data Breach Form.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A personal data breach that may result in a high risk to individuals may include where a parent is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then the School's Data Protection Officer must inform them of the breach by letter and make a formal apology. The School's Data Protection Officer will make the final decision as to whether notifying individuals is required.

Where pupils or parents are aware that they are the subject of a personal data breach, then they must be issued with a written apology. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

Where appropriate, remedial action should also consider anyone other than the pupil(s) or parent(s) who may also have been affected indirectly. These individuals should also be sent a written apology to minimise the School's reputational damage.

As well as the requirement to report personal data breaches to the ICO, it may also be necessary to report them to other authorities such as the police. These actions should only be undertaken following consultation with the Data Protection Officer.

6. Follow-up action

To ensure that we learn from our mistakes, the school is required not only to confirm that remedial action has taken place, but also that the causes of the personal data breach have been analysed and action taken to ensure similar breaches do not occur again.

7. Central logging of the issue

Once the school has confirmed remedial action and any appropriate follow-up action, then, subject to:

- the pupil(s) or parent(s) being satisfied with the remedial action taken in respect of the breach and;
- the Data Protection Officer being satisfied that regulatory procedures have been followed,

then the breach can be marked as closed by the Data Protection Officer.

A copy of all breach forms will be kept by the Data Protection Officer.

Appendix 4 – Data Breach – Incident Reporting Form

Please complete this form with as much detail as possible and email it to the School' Data ProtectionOfficer at head@bitterneceprimary.net (Unitl 31 Dec 2021) (Jan 2022 dscott-batey@springwellschool.net If you do not have sufficient information to complete all of the form, please complete everything you can and return it to the DPO as soon as possible and no later than 48 hours after you or the member of staff in your school became aware of the incident.

Part 1: Summary (TO BE COMPLETED BY THE DATA COMPLIANCE OFFICER)	
Name and department of person reporting:	
Date of report:	*[Please state the date you are completing the form]*
Time and date incident first identified by the school/staff member:	
Time and date incident occurred (if different):	
Circumstances of the incident:	*[Please give a summary of what actually happened]*
Part 2: Details of the personal data incident (TO BE COMPLETED BY THE DATA COMPLIANCE OFFICER)	
Nature of the incident:	[e.g. *which rules/procedures were breached and how did it happen? If you are not sure of the rules, just explain which internal procedure was not followed or ask the DPO for assistance]*
Categories of data subject affected:	[*e.g. pupils, parents, employee, others]*
Approximate number of data subjects affected (if known):	
Possible consequences	*[State if there is likely to be any detriment to*

of the incident for data subjects:	*individuals. If yes, please provide details]*
Part 3: Actions taken in response to the incident (TO BE COMPLETED BY THE DATA COMPLIANCE OFFICER IN CONJUNCTION WITH THE DATA PROTECTION OFFICER)	
What mitigating action was taken or will be taken in response to the incident?	
Follow up action taken to prevent similar future breaches	
Part 4: DPO actions (TO BE COMPLETED BY THE DATA PROTECTION OFFICER)	
Does the incident constitute a near miss or a personal data breach?	
If it is a personal data breach, is it notifiable to the ICO:	Y / N If Y, date notified If N, reason for not notifying the breach
If it is a personal data breach, is it notifiable to data subjects:	Y / N If Y, date notified If N, reason for not notifying the breach
Date issue closed:	