BLOSSOMFIELD

Infant and Nursery School
(incorporating Blossomfield Childcare)

Data Protection Policy

Eastcote Close, Shirley, Solihull
West Midlands, B90 3QX
Telephone: 0121 744 5522
Email: office@blossomfield.solihull.sch.uk

Reviewed internally for GDPR purposes – October 2024
Amends to clauses 1.2 and 18 – Approved by Governors on 27 November 2024
Next Review Date: SMBC Cycle

Data Protection Policy

BLOSSOMFIELD INFANT & NURSERY SCHOOL

(INCORPORATING BLOSSOMFIELD CHILDCARE)

1 Purpose

1.1 This policy sets out how all Staff and Governors at Blossomfield ensure that personal information is dealt with correctly and securely and in accordance with relevant Data Protection law ('the Law'), including the General Data Protection Regulations (GDPR), as well as related UK Data Protection legislation. In addition, this Policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 which gives parents the right of access to their child's educational record.

1.2 This Policy has also been written in conjunction with guidance from SMBC, Warwickshire Legal Services and the Data Protection Toolkit for Schools located within Keeping Children Safe in Education – September2024, clause 120.

1.3 This Policy should be read in conjunction with the Policies and Documents listed in Section 18 of this Policy.

1.4 A deliberate breach of this Policy will be treated as a disciplinary matter.

2 Roles and Responsibilities

2.1 The Data Protection Officer ('DPO') is responsible for providing advice and guidance to the School in order to assist the School to implement this Policy, monitor compliance with data protection law and develop related policies and guidelines where applicable. The DPO will carry out an annual audit of the School data processing activities and report to School their advice and recommendations on School data protection issues.

The DPO is also the first point of contact for individuals whose data the School processes and for the IOC. Our DPO is the School DPO Services and is contactable via Schooldpo@warwickshire.gov.uk or alternatively:

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick CV34 4RL

2.2 Solihull Metropolitan Borough Council Information Governance Team will advise on how long personal data can be held for and method of disposal. It is also available for advice relating to GDPR.

2.3 The School Governors are responsible for liaising with the Headteacher and School's Data Protection Champion in respect of any Subject Access Requests, approving relevant Policies relating to Data Protection and evaluating the progress of compliance with GDPR.

2.4 The Headteacher acts as the representative of the Data Controller on a day to day basis.

2.5 The School has nominated the following individual as the designated person to be contacted internally in relation to all matters relating to data protection issues (including access requests) and to make referrals, where necessary, to the Data Protection Officer: Linda O'Malley, Data Protection Champion, who is contactable via email: office@blossomfield.solihull.sch.uk or 0121 744 5522.

The Data Protection Champion will:

- Ensure she has the necessary resources from the DPO to fulfil her duties and maintain and expand her knowledge of GDPR.
- Ensure that any processing of personal data is only carried out if deemed necessary and for a specific purpose and that it is in line with the Data Protection principles set out in Data Protection Law (see section 4 of this Policy).
- Integrate Data Protection into internal documents (eg this Policy and any associated Policies and Privacy Notices).
- Provide or arrange for Staff and Governor Data Protection training as part of the induction process and part of continuing professional development where changes to legislation, guidance or the School's processes make it necessary.
- Maintain a record of School's processing activities.
- Make available to all Data Subjects (primarily via Privacy Notices), the name and contact details of School's DPO, the information School is required to share and how that data is used and processed.
- Maintain an internal record of all personal data (in relation to all categories of Data Subjects) held by the School, including details of the type of data held, the data source, the legal reason for processing, where/how the data is stored, security measures in place (including who has access to the data), who (if at all) the data is shared with external to the School, the legal reason for sharing the data externally and where the third party stores this data, how School ensures the data is accurate and up to date and how long it is retained.
- Maintain logs relating to completion of: Subject Access Requests, Personal Data Breaches, Data Destruction, Privacy Issue Dates, Data Protection Impact Assessments, Staff Training and general improvements to School systems improving compliance with GDPR.
- Ensure all internal and external documents relating to GDPR are regularly reviewed, updated and issued appropriately, offer regular training to existing and new staff and will provide regular reports/presentations to Governors and Headteacher on status of GPDR within School.

2.6 All members of Staff (including both permanent and temporary staff and volunteers) are responsible for:

- Collecting, storing and processing any personal data in accordance with this Policy.
- Informing the School of any changes to their own personal data, such as a change of address.
- Contacting the designated Data Protection Champion in the following circumstances:

    - With any questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this Policy is not being followed.
    - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual or transfer personal data outside the EEA.
    - If there has been a data breach.

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

3 Data Protection Law

3.1 The GDPR provides a framework for how organisations use personal information. It protects and enforces the privacy of personal information whilst also allowing for the lawful and appropriate use of this type of information about pupils, Staff, parents and others who have contact with the School.

3.2 The Law applies to many types of organisation processing personal information, including Schools. It covers all personal information regardless of its format or the way it is collected, used, recorded, updated, stored and destroyed.

3.3 Personal information relates to an individual who can be identified by that information or along with other information likely to come into a person's possession. The School acknowledges that the definition also covers opinions about an individual, information regarding the intentions of the School towards them, and more sensitive 'Special Categories' of information.

3.4 The GDPR is underpinned by a set of six straightforward principles and the School is committed to following these principles as set out in this Policy, Section 4.

3.5 In accordance with UK law, the School is registered as a Data Controller with the Information Commissioner's Office; the School will renew this annually.

Term	Definition
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Data Protection Impact Assessment (DPIA)	A risk assessment process designed to help analyse, identify and minimise the data protection risks of existing or proposed processing of personal data.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Personal Data	Any information relating to an identified, or identifiable, individual.

	This may include the individual's • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, alerting, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Subject Access Request (SAR)	The right of access allowing an individual to obtain records to their personal information, held by an organisation.

4 Processed Lawfully, Fairly and Transparently

4.1 In order to process data, the School must have a legal basis for doing so. The School must firstly consider if it can complete a task without the need for processing personal data by use of other reasonable means. If it cannot, then the School must identify the specific legal reason and be able to provide individuals with information about the lawful basis; this information can be incorporated into the School's Privacy Notices. Whilst there are six lawful reasons for processing personal data, schools are excluded from using number 6:

1 **Consent:** where the individual has given clear consent for the School to process their data for a specific purpose. This will only be used where other lawful bases would not be applicable.
2 **Contract:** where the process is necessary for a contract the School has with an individual or because the School has been asked to take specific steps before entering into a contract.
3 **Legal Obligation:** where the processing is necessary for the School to comply with law.
4 **Vital Interests:** where the processing is necessary to protect someone's life.
5 **Public Task:** where processing is necessary to perform a task in the public interest or School's official functions and the task or function has a clear basis in law.
6 **Legitimate Interests:** where processing is necessary for the organisation's legitimate interests or those of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This lawful reason will never be used by School.

Personal information which reveals any of the following is classified as 'Special Category' information, for which a separate set of rules governs whether this can be processed:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic and/or Biometric data
- Health information
- Information concerning a person's sex life or sexual orientation

The School will demonstrate why the law allows it to hold/share Special Category information. After the School has identified one of the legal bases above (from numbers 1-5), one of the following lawful reasons must **also** apply:

1 **Data Subject has given explicit consent:** this must have been provided by the data subject by way of a 'clear affirmative act' and not 'implied consent'. Written evidence of consent being made must be provided. Consent can be withdrawn at any time.

2 **Necessary for carrying out obligations and exercising specific rights in relation to employment and social security protection law:** this can be used in relation to staff information if a legal obligation requires the School, or a legal right enables the School, to hold particular information, so long as this is necessary.

3 **Necessary to protect vital interests of the Data Subject or another person where the Data Subject is physically or legally incapable of giving consent:** this is similar to Vital Interests above but can only be used where the person concerned is 'physically or legally incapable' of giving consent. This can be used in emergency situations where a person's life is in danger and vital information needs to be given to health staff, policy or fire crews and particularly in relation to health information relevant to emergency medical treatment.

4 **Processing relates to personal data which is manifestly made public by the data subject:** this is where the person concerned has published this information publicly, either on the internet or for general public consumption – not just for use by school. School will seek expert advice before selecting this basis.

5 **Necessary for establishing, exercising or defending legal claims:** only to be used when receiving legal advice or in relation to legal proceedings.

6 **Necessary for reasons of substantial public interest:** intended for protecting life or as a result of public interest investigations by media, police, government or others. It is very unlikely to be used by School.

7 **Necessary for preventive or occupational medicine:** this may be used by School in relation to assessment of an employee's working capacity and also in some circumstances relating to pupils (in less serious cases than the Vital Interests reason above). There must be a strong element of necessity for processing.

8 **Necessary for reasons of public interests in the area of public health:** this can be used if there are serious threats to health on a large scale.

4.2 Any personal data that School is required to hold, process or share will be communicated with that person(s) via Privacy Notices that will set out: the type of data, what the data is being used for, the legal reason for processing, who it is shared with, how long it will be stored, where it is stored and the rights of the Data Subject. Privacy Notices will also be published on the School website where relevant.

4.3 Where necessary, the School will conduct a Privacy Impact Assessment to ensure that it's processing of information does not pose a risk to the rights and freedoms of Data Subjects. This includes the introduction of new technologies; in this instance the School will take advice from the DPO.

5 Collected for Specified, Explicit and Legitimate Purposes

5.1 Personal information collected and held for purposes stated, will not be used for any other purpose without first informing those individuals whose data is being used and seeking further consent where necessary.

5.2 All School staff must only process personal data where it is necessary to do their job.

6 Adequate, Relevant and Necessary

6.1 School will only collect and store personal information that is sufficient for the purpose stated and will not ask for more information than is necessary.

6.2 School will regularly review its forms and check personal information already held for missing, irrelevant or excessive information.

7 Accuracy

7.1 Information held by the School will be as accurate and up to data as reasonably possible, with regular checking taking place. School will issue a pupil data checking sheet to all parents on an annual basis for this purpose.

7.2 If a Data Subject or any other person notifies School of a change of circumstances or an error in their personal data, the School will amend as soon as practicable.

8 Retention of Information

8.1 The School will not keep personal information for longer than is necessary for the stated purpose(s). In order to ensure this, all information held/created by the School (or held on its behalf), will be retained according to timescales set out in the Retention Schedule created by the Information Governance Team at Solihull Metropolitan Borough Council.

8.2 Personal data that is no longer needed will be disposed of securely and confidentially. Personal data that has become inaccurate or out of date will also be disposed of securely where the School cannot or do not need to rectify or update it. For example, the School will shred paper-based records and overwrite or delete electronic files. The School may also use a third party to safely dispose of records on its behalf but only where the third party can provide sufficient guarantees that it complies with Data Protection Law. Personal data contained in any document that needs to be retained longer, will be anonymised.

9 Access

9.1 Law enables individuals to exercise certain rights to enable them to access information held about them. There are a few exceptions to this rule but most individuals will be able to receive a copy of the information held on them. School acknowledges this and will follow the procedures set out in clause 9.3 below.

9.2 The specific rights given to individuals under law include:

- **The right to be informed** about data collection and use of their personal data at the time School collects that data.
- **The right of access** by an individual to their personal data. School will respond within one month.

- **The right of rectification** to personal data by way of amending or completing data where incomplete. These requests can be sent in writing or verbally and will be responded to within one month.
- **The right to erasure** of personal data. This right is not absolute – will only apply in certain circumstances. Requests can be made in writing or verbally and will be responded to within one month.
- **The right to restrict or suppress processing** of personal data. Restriction of processing allows School to still store personal data but would not be permitted to process it. These restrictions only apply in certain circumstances and requests should be by in writing or verbally with a response time of one month.
- **The right to data portability** allows individuals to obtain and re-use their personal data for their own purposes by allowing them to copy or transfer their information from one IT environment to another. This only applies to information the individual has already supplied to School.
- **The right to object** allows individuals to object to the processing of their information. If School has a compelling reason to process the information, the request may be rejected except where consent was originally sought. Objections can be in writing or verbally and will be responded to within one month.
- **Rights in relation to automated decision making and profiling.** This is highly unlikely to be used by School and there are certain restrictions in place to prevent its mis-use.

9.3 Where an individual has made a Subject Access Request, to gain access to personal information that the School holds about them, this will include:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of data, if not the individual
- Whether any automated decision-making is being applied to their data and what the significance and consequences of this might be for the individual

Subject Access Requests may be submitted in writing (by letter or email) or verbally, to the Data Protection Officer, a member of Staff or Governor. To enable the request to be accurately responded to, the applicant should be encouraged to make the request in writing and to set out the:

- name of the individual
- name of the School
- correspondence address
- contact number and email address
- details of the information requested

Where the Subject Access request has been sent to the DPO, the DPO will forward the Subject Access Request to the School's Data Champion. If a member of Staff receives a

Subject Access Request, they must also send it directly to the School's Data Champion. Information to be released will be collated by the School's Headteacher and Data Champion and the DPO will be informed of such request.

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer to make a Subject Access Request with respect to their child, the person should have parental responsibility for the child and the child must either be unable to understand their rights and the implications of a Subject Access Request, or have given consent. Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, Subject Access Requests from those with parental responsibility for pupils at our School will, in general, be granted without the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case by case basis.

9.4 When responding to Subject Access Requests we:

- may ask the individual to provide two forms of identification
- may contact the individual via telephone to confirm the request was made
- will respond without delay and within one month of receipt of the request
- will facilitate the request to provide information free of charge but are at liberty to charge a reasonable fee for additional copies of information (for time, printing and posting)
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to School closure. We will inform the individual of this within one month and explain why the extension is necessary

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parent order records
- is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

9.4 The School also acknowledges that the Education (Pupil Information) (England) Regulations 2005) gives parents/guardians rights to their child's educational record (which includes most information about a pupil). The School will respond to such requests within 15 school days of receipt of a written request.

10 Security

10.1 The School will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

10.2 Paper-based records and portable electronic devices such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

10.3 Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards or left anywhere else where there is general access.

10.4 Staff must ensure that passwords are difficult for anyone else to guess; incorporate numbers and mixed cases.

10.5 Encryption software is used to protect all portable devices and removal media on which personal information is stored, such as laptops and USB devices.

10.6 Staff, Pupils and Governors, who store personal information on their own personal devices, must follow the same security procedures as for school-owned equipment.

10.7 Where personal data needs to be shared with a third party, carry out due diligence and take reasonable steps to ensure the data is stored securely and is adequately protected.

10.8 Refer to School's Information and Security Policy for additional guidance.

11 Personal Data Breaches

11.1 The School shall take all reasonable steps to ensure that there are no personal data breaches.

11.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

11.3 When appropriate, the School shall report the data breach to the ICO within 72 hours. Such breaches in a School context may include, but are not limited to:

- a non-anonymised dataset being published on the School website of pupils eligible for pupil premium
- safeguarding information being made available to an unauthorised person
- the theft of a School laptop containing non-encrypted personal data about pupils

12 Sharing Personal Data

The School will not normally share personal data with any parties not included in its Privacy notices. However, GDPR and DPA 2019 also allow information to be shared where:

- The safety of Staff is put at risk by a pupil or parent
- The School needs to liaise with other agencies but will seek consent as necessary
- another organisation provides School with a service that is required to carry out its Public Tasks. In this instance, School will:

12.1 have entered into a written contract with the organisation acting as a Data Processor on behalf of the School. Existing contracts already in place will be checked by School to ensure they comply with the new GDPR legislation. If any contracts do not comply, a standard letter approved by the DPO will sent out by School to the Data Processor. Should the Data Processor object to the standard clauses being incorporated into the contract, the matter will be referred by School to the DPO. Absence of objection from a Data Processor is taken as agreement to include the clauses at the end of the existing contract.

12.2 Any contracts in existence between the School and an external Data Processor, where data is transferred outside of the EEA, will be referred to the DPO to ensure that those countries are providing an equivalent level of data protection under their own legislation.

12.3 School also shares information where no formal contract is in place; this is usually where sharing information is due to legal obligations, eg to the Local Authority and Department of Education. In these instances, the School will send out a Data Sharing Agreement requesting the organisation to sign and return. Whilst sharing information without entering into such an Agreement is not unlawful, it is good practice to record such arrangements in formal terms.

12.4 The Data Sharing Agreement makes it clear that both parties will comply with GDPR and other relevant legislation to ensure that information is being lawfully and securely transferred.

12.5 Parties to the Agreement are also expected to assist each other through a mutual assistance clause (for example, in relation to data breaches).

12.6 External organisations may also process School data where no contract is in place. Where this is identified by School, a Data Processing Agreement will be sent to the organisation requesting them to sign up.

12.7 Records of checks of adequate security and documentation sent out to Data Processors will be maintained and regularly reviewed by School.

12.8 Personal data may also be shared with third parties for research and statistical purposes. In such circumstances, all personal data will be anonymised or consent will be sought.

13 Photographs and Videos

13.1 The School will seek parental consent to use certain types of personal information where appropriate. Examples include seeking consent for including photographs or recordings of children in School for School projects or for display; using photographs of children, Staff and parents in School publications such as newsletters; using photographs of children, Staff and parents in external publications such as a local newspaper; using photographs/recordings of children, Staff and parents to be on any web page or social media site.

13.2 When using photographs and videos within School, we will not accompany them with any other personal information about the child to ensure they cannot be identified by visitors in School. See our Safeguarding Policy for more information on our use of photographs and videos.

13.3 When collecting consent, the School will provide a clear explanation of the use of the information and will ask for a positive written indication of consent for each different use. Consent will not be inferred from a non-response to a communication, for example from a parent's failure to return or respond to a letter.

13.4 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

14 Public Displays

14.1 If there is a display of pupils' work to be shown at a public venue, (other than on the School premises), parents will be informed. Unless the School has consent from the Parent to publish fuller information, the School will only include the minimum of pupil identifiable information, for example "by John, year 1".

15 School Plays

15.1 Data Protection law does not prevent parents/guardians from capturing their child's performance on camera or video as these instances would be for personal/family use only and therefore Data Protection law does not apply.

16 Review

This Policy will be reviewed and updated as necessary to reflect best practice and/or in accordance with any amendments made to Data Protection Law.

17 Complaints

Complaints will be dealt with in accordance with the School's Complaints' Policy. Complaints relating to information handling may also be made to the Information Commissioner's Office.

18 Links to Other Policies and Documents

This Policy should be read in conjunction with the School's:

- Information Security Policy
- Freedom of Information Policy
- Confidentiality Policy
- Complaints' Policy
- Safeguarding Policy
- School Use of Personal and Social Communication Tools
- Use of Mobile Phones and Image Capturing Devices
- Privacy Notices
- Keeping Children Safe in Education – September 2021– Data Protection Toolkit for Schools

Appendix 1: Personal Data Breach Procedures

If you become aware that information has not been handled according to procedure and there is a data breach or potential security incident, you must report it in accordance with the procedure below.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of GDPR.

1 Data protection breaches occur where personal data is lost, damaged, destroyed stolen, misused and/or accessed unlawfully.

2 Examples of how a breach may occur include:

a Theft of data or equipment on which data is stored
b Loss of data or equipment on which data is stored
c Inappropriate access controls allowing unauthorised use
d Accidental loss
e Destruction of personal data
f Damage to personal data
g Equipment failure
h Unlawful disclosure of personal data to a third party
i Human error
j Unforeseen circumstances such as fire or flood
k Hacking attack
l 'Blagging' offences where information is obtained by deceiving the organisation which holds it

3 If any member of Staff discovers that data has been lost, or believes there has been a breach of the data protection principles in the way that data is handled, he/she must immediately – or not later than 24 hours of first coming to notice – inform the School's Data Protection Champion (Linda O'Malley). **If this occurs outside of School hours or during School holiday periods, it should be reported to Mrs Farkas, Headteacher using the contact numbers on the Cascade list.**

4 Upon being notified, the School's Data Protection Champion will assess whether a breach of personal information has occurred and the level of severity. If breach has occurred, but the risk of harm to any individual is low (for example, because no personal information has left the control of the School, then the School's Data Protection Champion will undertake an internal investigation to consider whether the Information Security Policy was followed and whether any alterations need to be made to internal procedures as a result.

5 In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate/minimise the risk to those individuals affected by it.

All School Staff and Governors are expected to work in partnership with the Data Protection Champion and the Data Protection Officer in relation to the following matters:

Notification of Breaches

Any members of Staff or Governor who becomes aware of a personal information breach should provide full details to the Data Protection Champion for the School within 24 hours of being made aware of the breach. The Data Protection Champion will then complete the Data Breach Record Form and Incident Log.

When completing the form, details should be provided of the reporter's name, the date and time of the breach, the date and time of detecting the breach and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and compile a recovery plan, including damage limitation. Input may be required from specialists such as IT, HR and Legal; in some cases, contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recover of released documents, finding a lost piece of equipment or simply changing any related access codes.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- In addition to the physical recover of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that Staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified.

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a pupil file is lost then risks are different depending on the type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Champion should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data have been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, financial loss or a combination of these and other aspects of their life?
- Are their wider consequences to consider such as a risk to life?
- Loss of public confidence in the School?

All Staff and Governors should establish whether there is anything they can do to recover any loses and limit the damage the breach can cause.