EAST BARNET SCHOOL

"I want to learn"

Data Protection Policy

(Including SAR, Data Breach, Information Security Appendices)

Version 1.4

Reviewed by Resources Committee:	November 2025
Adopted by Governing Body:	March 2026
Reviewer:	H. Chamberlain
Governor Link:	Chair of Resources

DATA PROTECTION POLICY

East Barnet School, Chestnut Grove, East Barnet, Herts EN4 8PU

Introduction

The UK General Data Protection Regulation (UK UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The school will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the school's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

A. Definitions

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can

reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.
Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller

The organisation storing and controlling such information (i.e. the school) is referred to as the Data Controller.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

B. When Can the School Process Personal Data?

Data Protection Principles

The school are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR.

The principles the school must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The school only collect, process and share personal data fairly and lawfully and for specified purposes. The school must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The school may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);

- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the school's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The school may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the school in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The school identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the school relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them.

Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented 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 will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the school will normally seek another legal basis to process that data. However if explicit consent is require the data subject will be provided with full information in order to provide explicit consent.

The school will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The school will not 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 purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The school will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the school shall delete or anonymise the data. Please refer to the school's Data Retention Schedule for further guidance.

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The school will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the school.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The school will ensure that they adhere to legal timeframes for retaining data. We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the school's Retention Policy for further details about how the school retains and removes data.

Principle 6: Personal data must be 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

In order to assure the protection of all data being processed, the school will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the school replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The school follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.
The school will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.
Full details on the school's security measures are set out in the school's Security Policy.

Sharing Personal Data

The school will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the school is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, 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.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.
The school will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the school's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

C. Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.
The rights data subjects have in relation to how the school handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the school's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);

(d) Prevent our use of their personal data for 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) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) 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.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the school to verify the identity of the individual making the request.

Direct Marketing

The school are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The school will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The school will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the school in the course of their employment or engagement. If so, the school expects those

employees to help meet the school's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Please refer to the school's Security Policy for further details about our security processes;
- Not to remove personal data or devices containing personal data from the school premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

D. Accountability

The school will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The school have taken the following steps to ensure and document UK GDPR compliance: -

Data Protection Officer (DPO)

Please find below details of the school's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the school to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed but would refer you to the school's data retention schedule in the first instance;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach and would refer you to the procedure set out in the school's breach notification policy;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The UK GDPR requires the school to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

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. Immediately contact the person designated as the key point of contact for personal data breaches (Head of IT Services) or your DPO.

Transparency and Privacy Notices

The school will provide detailed, specific information to data subjects. This information will be provided through the school's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the school use their data and the school's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the school's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The school will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the UK GDPR

Privacy by Design

The school adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.
Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the school takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the school conduct DPIAs for any new technologies or programmes being used by the school which could affect the processing of personal data. In any event the school carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The school are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the school;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the school's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The school will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The school, through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually/regularly in order to review use of personal data.

Related Policies

1. Data Retention Policy
2. Data Security Policy
3. Data breach notification policy
4. Privacy Notices

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the school.

SUBJECT ACCESS REQUEST APPENDIX 1

East Barnet School, Chestnut Grove, East Barnet, Herts EN4 8PU

Subject Access Request

Under Data Protection Law, Data Subjects have a general right to find out whether the school hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the school are undertaking.

A Data Subject has the right to be informed by the school of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the school's sources of information obtained;

(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the school process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school hold about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to School Business Leader who should contact Judicium as DPO in order to assist with the request and what is required.

Acknowledging the request

When receiving a SAR the school shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the school may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information; and/or

- consent (if requesting third party data).

The school should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the school will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the school has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before responding to the request.
In both cases, the period of responding begins when the additional information has been received. If the school do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The school may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their

rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the school is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the school will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested.

Time Period for Responding to a SAR

The school has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because the school will be closed/no one will be on site to comply with the request/our mail gets forwarded/ we do not review emails during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request we may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her.
The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained.
The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.
The information that the school are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the school have one month in which to respond the school is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR. The school is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the school need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The school will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the school do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or

- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The school do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The school do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the school receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another

individual (i.e. the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The school do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The school do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The school do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

DATA BREACH APPENDIX 2

East Barnet School, Chestnut Grove, East Barnet, Herts EN4 8PU

A. Introduction

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data. The GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the school of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the school's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

B. Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

C. Special Category Data

Previously termed “Sensitive Personal Data”, Special Category Data is similar by definition and refers to data concerning an individual’s racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

D. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

E. Data Subject

Person to whom the personal data relates.

F. ICO

ICO is the Information Commissioner’s Office, the UK’s independent regulator for data protection and information.

G. Responsibility

Head of IT Services or School Business Leader has overall responsibility for breach notification within the school. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.
In the absence of Head of IT Services or School Business Leader, please contact any other member of the IT Department.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below:

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

H. Security and Data-Related Policies

Staff should refer to the following policies that are related to this data protection policy: -

The Security Policy which sets out the school's guidelines and processes on keeping personal data secure against loss and misuse.

The Data Protection Policy which sets out the school's obligations under GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found on the school's website and the EBS Staff Hub Intranet.

I. Data Breach Procedure

What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop, memory stick or a paper file (this includes accidental loss);

- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When Does It Need to Be Reported?

The school must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a data breach report form (which can be obtained from the Head of IT Services;
- Email the completed form to Head of IT Services or Business Manager.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the school and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights

and freedom of individuals. They can seek advice from their line manager, Head of IT Services, a member of SLT or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. Head of IT Services or School Business Leader will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, Head of IT Services or School Business Leader will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to: -

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the school's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

Head of IT Services or School Business Leader will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the school are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Head of IT Services or School Business Leader will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the school have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Head of IT Services or School Business Leader will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the school will consider alternative means to make those affected aware (for example by making a statement on the school website).

Notifying Other Authorities

The school will need to consider whether other parties need to be notified of the breach. For example:

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, the school will carry out all necessary investigations into the breach.

The school will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the school will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the school will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to IT Department or the DPO. This can help capture risks as they emerge, protect the school from data breaches and keep our processes up to date and effective.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the school.

INFORMATION SECURITY APPENDIX 3

East Barnet School, Chestnut Grove, East Barnet, Herts EN4 8PU

---

1. Statement of Principle

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data. The School is committed to ensuring the security of all information that it holds and will implement the highest standards of information security.

1.1 This document sets out the measures in place to:

- protect against potential breaches of confidentiality
- ensure that all information assets and IT facilities are protected against damage, loss or misuse
- support our Data Protection Policy in ensuring all staff are aware of and comply with both UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements for information security and the responsibility placed on all staff to protect the confidentiality and integrity of the information that they personally handle.

2. Introduction

2.1 Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

2.2 Staff are referred to the School's Data Protection Policy and Data Breach Policy for further information. These policies are also designed to protect personal data and can be found within the HUB.

2.3 For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

3. Scope

3.1 The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, on whatever medium. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

3.2 This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

3.3 All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Breach of this policy by staff will be treated as a disciplinary offence which may result in action under the School's Disciplinary Policy and Procedure, up to and including summary dismissal depending on the seriousness of the breach.

3.4 This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

3.5 Breach of this policy by others, including Governors, temporary staff, or contractors will be dealt with as deemed appropriate by the Chair of Governors or Headteacher and may be reported to the police.

4. General Principles

4.1 All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further

details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

4.2 Staff should discuss with their line manager the appropriate security arrangements for the type of information they access in the course of their work. Contractors, volunteers and interns should discuss this with their primary contact point in the school. The Chair of the Governors is responsible for ensuring that all governors are aware of and respect appropriate security arrangement for information entrusted to them.

4.3 All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption. Data subjects have a right to request information held about them (see Data Protection Policy.) Interns, volunteers and governors should be given access by staff to the information required by them to fulfil their agreed duties and responsibilities.

4.4 All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the IT Department.

4.5 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Network Manager unless expressly stated otherwise.

4.6 All staff, volunteers, interns and governors have an obligation to report actual and potential data protection compliance failures to the School Business Leader/ Network Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

4.7 The Data Link Governor will be notified of minor breaches and potential breaches termly, and immediately in the case of a serious breach which may need to be reported to the Information Commissioners Office (ICO).

5. Physical Security and Procedures

5.1 Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows.

5.2 To avoid unauthorised or accidental access, all paper documents shall be securely locked away at the end of the working day, when they are not being used, or when the room or desk is left unoccupied.

5.3 Available storage cupboards or locked cabinets shall be used to store paper records when not in use.

5.4 Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained.

5.5 Particular care must be taken if documents have to be removed from the school.

5.6 The physical security of buildings and storage systems shall be reviewed on a regular basis. If the security is found to be insufficient, the person discovering this must inform the School Business Leader as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

5.7 The School carries out regular checks of the buildings and both physical and data storage systems to ensure they are maintained to a high standard.

5.8 The School has an intercom system to minimise the risk of unauthorised people entering the premises and closes the perimeter gates during certain hours to prevent unauthorised access to the grounds. An alarm system is set nightly.

5.9 CCTV Cameras are in use at the School and monitored by the Premises Team. Recordings are made for the safety and protection of those on the site and to aid detection of crime.

5.10 Visitors should be required to sign in at the reception. They must never be left alone in areas where they could have access to confidential information unless such access has been agreed to be necessary to the visit.

6. Computers and IT

Responsibilities of the IT Manager

The IT Network Manager shall be responsible for the following:

6.1 ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;

6.2 ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;

6.3 along with the Headteacher, ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

6.4 Furthermore, the IT Network Manager shall be responsible for the following:

6.5 assisting all members of staff in understanding and complying with this policy;

6.6 providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;

6.7 ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;

6.8 receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];

6.9 taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;

6.10 monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and

6.11 ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of Staff (including Governors, Interns and Volunteers)

6.12 All users must, at all times comply with all relevant parts of this policy when using the IT Systems.

6.13 Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

6.14 All users must immediately inform the IT Network Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

6.15 Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems must be reported to the IT Department immediately.

6.16 Users are not entitled to install onto school systems any software they own, have obtained or provided without permission. Prior to installation, staff must obtain written permission from the IT Network Manager. This permission must clearly state the name of the software, and onto which computer(s) or device(s) it may be installed.

6.17 Furthermore, any such software must be approved by the IT Network Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

6.18 Physical media (e.g. USB memory sticks or data storage disks of any kind) must be virus-scanned before using it to transfer files. Approval from the IT Network Manager must be obtain prior to transferring of files using external cloud storage systems.

6.19 If a user detects any potential or actual virus, this must be reported immediately to the IT Network Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

System Access Security

6.20 All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

6.21 The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

6.22 All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods (e.g., finger prints) can only be used if approved by the IT Department.

6.23 All passwords must, where the software, computer, or device allows:

- be at least 6 characters long including both numbers and letters
- be changed on a regular basis (and at least every 180 days)
- cannot be the same as the previous 10 passwords you have used
- not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.)

6.24 Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the IT Network Manager as appropriate and necessary.

6.25 Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

6.26 Any member of staff who discloses their password to anyone, other than a member of I.T., in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure.

6.27 Any member of staff who logs on to a computer using another member of staff's password or accesses the device when it has been left unlocked, will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

6.28 If you forget your password, you should notify the IT Department to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

6.29 You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

6.30 School computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) must be protected with a screen lock that activates after a period of inactivity. You may not change this time period or disable the lock.

6.31 All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not change this time period or disable the lock.

Data security

6.32 Personal data sent over the school network must be encrypted or otherwise secured.

6.33 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior written authorisation from the IT Network Manager, who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems and opened or run.

6.34 Staff, Governors and visitors may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided the relevant requirements and instructions governing this use are followed.

6.35 All usage of 'own device(s)' whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The IT Network Manager may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

6.36 All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the IT Department.

6.37 All data stored electronically on portable physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

6.38 Staff should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Headteacher. Where permission is given, any new or changed data must be copied back onto the School's computer network in order for it to be stored and backed up. Personal data on mobile devices must be deleted as soon as any need for its retention has passed

6.39 All electronic data must be securely backed up by the end of the each working day and is done by the IT Department.

7. Off-Site Working

7.1 Where staff are taking confidential information off-site, they must be satisfied that appropriate technical and practical measures are in place at the home or other remote location and on the journey between school and off-site to maintain the continued security and confidentiality of that information.

7.2 When someone has been given permission to take confidential or other information off-site, they must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

- all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

8. Communications, Transfer, Internet and Email Use

8.1 When using the School's IT Systems users are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

8.2 The School works to ensure the systems to protect pupils and staff and are reviewed and improved regularly.

8.3 Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee, and the school cannot accept liability for the material accessed or its consequence.

8.4 If staff, visitors or pupils discover unsuitable sites or any material which would be deemed unsuitable or illegal, this should be reported to the Safeguarding Officer or I.T. Network Manager or their team.

8.5 All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery.

8.6 Postal, DX, email addresses and numbers should be checked and verified before information is sent. In particular extra care must be taken when adding email addresses, where auto-complete features may have inserted incorrect addresses or recipients.

8.7 Do not reply to emails using 'reply to all' before checking that everyone on the recipient list should be seeing the reply.

8.8 Do not forward emails without checking if email addresses and personal information in the body of the email need to be deleted or not.

8.9 You should be careful about maintaining confidentiality when speaking in public places.

8.10 Confidential information should be marked 'confidential' and only circulated to those who need to know the information in the course of their work for the School.

8.11 Personal or confidential information should not be removed from the School without prior permission from the Headteacher except where the removal is temporary and necessary. When such permission is given the bearer must take all reasonable steps to ensure that the both the integrity and the confidentiality of the information are maintained. To this end, the information:

- must not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

9. Reporting Security Breaches

9.1 All members of staff have an obligation to report actual or potential data protection compliance failures.

9.2 All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the IT Network Manager.

9.3 When receiving a question or notification of a breach, the IT Network Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

9.4 Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the IT Network Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, IT Network Manager.

9.5 Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the School Business Leader.

9.6 All IT security breaches shall be fully documented and reported termly to the Data Link Governor.

9.7 Full details on how to notify of data breaches are set out in the Breach Notification Policy.

10. Related Policies

10.1 Staff should refer to the following policies that are referenced in this Information Security Policy:

- Data Breach Policy
- Data Protection Policy