Data Protection Policy

Code: S11

Date of approval: 14th January 2022

Date of next review: Spring 2023

Agreed by Whitchurch Primary School Governing Body	Name
Chair of Governing Body	Paul Smith
Headteacher	Caroline Rowley

Version	Date	
1	March 2022	New Policy

Introduction

The United Kingdom General Data Protection Regulation (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 GPDR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy meets the requirements of the UK GPDR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GPDR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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.

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.

SECTION 1 – 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.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

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 and could include DBS checks.

SECTION 2 - 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 GPDR.
The principles the School must adhere to are: -

(a) Personal data must be processed lawfully, fairly and in a transparent manner;
(b) Personal data must be collected only for specified, explicit and legitimate purposes;

(c) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
(d) Personal data must be accurate and, where necessary, kept up to date;
(e) 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; and
(f) 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.

Further details on each of the above principles is 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 GPDR.
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; or
- 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 a 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; or
- 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 GPDR.

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 required 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 GPDR.

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 the data 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.

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. Full details as to how to make this request are detailed within the Schools Privacy Notice.

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; and
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follows 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 Privacy Notice.

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 GPDR 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.

Biometric recognition systems

Were we to use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.
Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.
Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.
Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s). Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.
Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
Any enquiries about the CCTV system should be directed to the School Business Manager.

Photographs and videos

As part of some school activities, staff may take photographs and record images of individuals within the school. Written consent from parents/carers for photographs and videos will be obtained prior to such usage.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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. Images used will be pseudonymised where possible.

Transfer of Data Outside the European Economic Area (EEA)

The UK GPDR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GPDR 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 GPDR. 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.

SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and the school's Privacy Notice 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;
(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.

Subject Access Requests

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; and
(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.
(h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request. For further information, please refer to:

- Appendix 1: Subject Access Request Policy
- Appendix 2: Subject Access Request Form
- Appendix 3: Subject Access Request – pupil record
- Appendix 4: Personal Data Breach procedure

The request should in the first instance be sent to office@whitchurchprimary.harrow.sch.uk.

Direct Marketing

The School is 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 and
- 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; and
- Not to store personal information on local drives.

Children and subject access requests

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 child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 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 parental 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.

Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

SECTION 4 – ACCOUNTABILITY

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. The school is responsible for and demonstrate accountability with the UK GPDR principles.
The School have taken the following steps to ensure and document UK GPDR compliance: -

Data Protection Officer (DPO)

Please find below details of the School's 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

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 GPDR 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 Privacy Notice 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 Data Protection 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; or
(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 GPDR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

We have put in place procedures (See Appendix 4) 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 School Business Manager via office@whitchurchprimary.harrow.sch.uk

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 GPDR 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 publically 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 GPDR.

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 GPDR

Privacy by Design

The School adopt a privacy by 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 GPDR 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; or
- 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 regularly in order to review use of personal data.

SECTION 5 - Roles and responsibilities

This policy is applicable to all staff employed by the school, and to external organisations or individuals working on the school's behalf.
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.

Governing body

The Governing Body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Headteacher

The head teacher acts as the representative of the data controller on a day-to-day basis.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
The DPO is also the first point of contact, via the school's data protection lead (DPL) for individuals whose data the school processes, and for the ICO.

Our DPL, School Business Manager, is contactable via office@whitchurchprimary.harrow.sch.uk or on the address below:

Data Protection Officer:
Judicium Consulting Limited:
72 Cannon Street, London,
EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174

All staff

Staff are responsible for:
Collecting, storing and processing any personal data in accordance with this policy;
Informing the school of any changes to their personal data, such as a change of address;
Contacting the DPO via the Data Protection Lead 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 European Economic Area
- 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.

Remote Access Agreement

This agreement sets out guidelines and requirements which must be adhered to when accessing they school's systems and data remotely. These are to reduce the risks associated with digital data such as plagiarism, theft, data corruption and data breeches. Realisation of these risks through the misuse and non-compliance of remote access procedures places remote access users in breach of moral, ethical, legislative or contractual obligations. This agreement should be read in conjunction with the school's data protection policy.

Definition:

Remote Access – Accessing the Whitchurch Primary School & Nursery network, including SIMS, from outside of the premises via a different network through the use of a configured Whitchurch Primary School & Nursery laptop or device.

Scope & limitations

- The Whitchurch Primary School & Nursery remote access policy applies to all remotely accessible systems and data controlled by the school.
- The school does not make provision for all its systems and services to be made available remotely to all users with remote access permission.
- With regard to availability and speed of remote access services, it should be borne in mind that these may be reliant on 3rd party factors such as the user's Internet Service Provider connectivity and domestic networking hardware such as routers.
- The privilege of remote access is at the discretion of the Head Teacher and access is dependent on their current role and permissions.

User responsibilities and good working practices

- To know what information they are accessing, using or transferring
- To understand and adhere to contractual, ethical or other requirements attached to the information and pertinent to the school's policies and procedures
- To be responsible for following correct procedures when logging out of the remote session

Responsibilities for data/information accessed and/or processed during mobile working

- Confidential data/information should not be created, stored or processed on privately owned computers.
- 3rd party devices should not be considered or assumed to be secure and the use of such devices for storing documents or other work related to the school is discouraged, Whitchurch Primary School & Nursery systems that have been allocated to staff have strong controls and are configured to protect the integrity of the data.
- Appropriate precautions and good practice should be followed for all data and information that has been edited, created and/or saved on mobile or home devices or other forms of media, e.g. viewing attachments from work email accounts on mobile phones.

Security of Whitchurch Primary School & Nursery's owned computers or other mobile devices

When using systems and devices owned by the school to perform work for Whitchurch Primary School & Nursery and it is considered that access is secure, users should still:

- Return the device to the Operations Manager for system faults, system security updates and patches or any other security related issues.
- Maintain safe web-surfing practice.
- Change passwords regularly and follow Whitchurch Primary School & Nursery's password policy – 8 digits, to include an upper and lower case letter plus a number and special character such as # & @
- Devices are not left unattended, even for short period of times, without locking the screen, and never in public places.
- Data that is deemed confidential is not left visible on the screen where others are able to see it.
- Not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.

Return of assets to Whitchurch Primary School & Nursery

- All systems and devices, plus information/data owned by Whitchurch Primary School & Nursery must be returned to the school upon termination of employment or contract.
- Before returning the devices, users should remove their own personal data from the system.

Removal of remote access rights

- Access rights for remote access may be changed or removed by Whitchurch Primary School & Nursery from any authorised/unauthorised user at any time if a breach of the conditions of use has been performed or that user's access is compromising the confidentiality, integrity and/or availability of Whitchurch Primary School & Nursery's systems or services.
- The remote access rights of all employees and third party users shall be removed upon termination of employment, contract or agreement.

Reporting a data breach

Should there be a loss of data which identifies an individual, staff/pupil/parent, the Data Protection Lead must be notified immediately. This includes the loss of hard documentation, an error in sending an email, loss/theft of IT equipment, someone getting access to data from your device through phishing, etc. The DPL will notify the school's DPO who will decide if this breach is reportable to the Information Commissioner's Office. (please see the Data Protection Policy for further details)

Signed: Date:

Name: Job Title:

Related Policies

This Policy should be read with reference to the following policies that are related to this data protection policy: -

- Privacy Notice
- Safer Recruitment Policy
- Acceptable Use Policy
- Freedom of Information Publication Scheme
- Staff/Pupil Mobile Phone Policy

These policies are also designed to protect personal data and can be found within the School's Intranet.

Appendix 1: Subject Access Request Policy

Introduction

The School, Whitchurch Primary School & Nursery, holds personal data (or information) about job applicants, employees, pupils and parents and other individuals for a variety of purposes.

Under Data Protection Law, individuals (known as 'data subjects') have a general right to find out whether the School holds or processes 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 is undertaking.

This policy provides guidance for staff members on how data subject access requests should be handled, and for all individuals on how to make a SAR.

Failure to comply with the right of access under the GDPR puts both staff and the School at potentially significant risk, and so the School takes compliance with this policy very seriously.

If you have any questions regarding this policy, please contact our Operations Manager or the School's DPO whose details are as follows:

Data Protection Officer: Craig Stilwell

Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Telephone: 0203 326 9174

Definitions

- **Data Subjects** for the purpose of this policy this includes all living individuals about whom we hold personal data. This includes pupils, our workforce, and other individuals, such as governors and volunteers. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
- **Personal Data** means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties

How to recognise a Subject Access Request (SAR)

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 processes 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 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 all the information that you have 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 to 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 use the School’s form at Appendix 1 and 2 of the policy. This allows the School to easily recognise that you wish to make a data subject access request.

What to do when you receive a data Subject Access Request
All data subject access requests should be immediately directed to our Operations Manager who will contact the DPO for assistance if needed. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner’s Office (ICO) and/or legal action by the affected individual. So it is crucial to ensure that requests are passed to the relevant individual without delay and failure to do so may result in disciplinary action being taken.

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 to respond to the request. In addition to acknowledging the request, the School may ask for proof of ID if needed or 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.

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 that 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.

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. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request. A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.
If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

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

In circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester, the written authorisation of the data subject 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 will not be able to be responded to within the one calendar month response period. This is because the School will be closed and there may not be anyone on site to comply with the request or to review emails during this period. As a result, it is unlikely that your request will be received during this time (and so the time period does not run until we receive the request). We may not be able to acknowledge your request during this time (i.e. until a time we receive the request) and the time period may not start 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 and the following information:

- the purposes for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
  - to request that the Company rectifies, erases or restricts the processing of his personal data; or
  - to object to its processing;
  - to lodge a complaint with the ICO;
  - where the personal data has not been collected from the individual, any information available regarding the source of the data;
  - any automated decision we have taken about him or her (see paragraph 9 below), together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for 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 is 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.
Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors e.g. LA providers;
- occupational health records held by the Occupational Health Department;
- pensions data held by LA Payroll Services.
- data held by its HR consultants, London Borough of Harrow and HT consultant for Performance Management.
- SIMS, Evolve, LGFL

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Requests made by third parties
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.
If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Requests made on behalf of children
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.

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 individual's 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.

Refusing to respond to a request
The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision. The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record keeping
A record of all subject access requests shall be kept by the School Business Manager. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

Appendix 2: Subject Access Request form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of identity: We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

A copy of the below form is available on the school website.

Section 1
Please fill in the details of the data subject (i.e. the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth Certificate
- ☐ Driving Licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information *If you only want to know what information is held in specific records. please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*
Details:

Employment records: *If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your Staff number/Unit/Team/Dates of employment.*
Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth Certificate
- ☐ Driving Licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g. parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (time period/ categories of data/ information relating to a specific case/ paper records/ electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to:
office@whitchurchprimary.harrow.sch.uk

Appendix 3: Subject Access Request – pupil record

If you would like request information about your child, please complete the following form which is also available on the school website.

Dear School Business Manager,

Please provide me with information about my child, who is under the age of 12yrs, that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about him/her, and verify the lawfulness of the processing.
Below are the details required:

Name:	**Date:**
<u>Relationship with school</u> Please select: Pupil / parent / employee / governor / volunteer Other (please specify):	
Name of child	
Registration Group	
Relationship to the child	
Correspondence address	
Contact number	
Email address	
Details of the information requested: Please provide me with: *(Insert details of the information you want that will help us to locate the specific information)*	Please be as precise as possible, e.g.: My child's *(Insert Name)* medical records My child's *(Insert Name)* behaviour record, held by *(Insert class teacher Name*) Emails between 'A' and 'B' between *(dates)*

If you need any further information, please inform me as soon as possible. Please bear in mind that under the UK GPDR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

Yours sincerely,

Name

Appendix 4: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioners Office (ICO).
On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Lead (School Business Manager) who will in turn notify the Data Protection Officer (DPO).
The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Management drive on the school's network.
Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached.

This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the Management drive on the school's network.
The DPL and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches
The school will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The school will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must inform the school's Data Protection Lead (DPL) immediately.
- Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error.
- The DPL will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPL will seek advice from the DPO and will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Sensitive information being disclosed via a school laptop or IT equipment containing non-encrypted sensitive personal information being stolen or hacked

- The member of staff who is allocated that item must report this to the DPL immediately.

- The DPL will report this to the Head Teacher, DPO and Chair of Governors. Police will also be notified, with the hope that the equipment may be recovered.
- Any personal data which might have been released is identified and potential consequences will be assessed and mitigated.
- DPO will support the school in recording and reviewing the breach and school procedures including actions which need to be taken to reduce the risk of this happening again.

Sensitive information being disclosed via the loss of a hard copy of information being stolen or misplaced in a public place.

- The member of staff who discovers this loss must report this to the DPL immediately.
- The DPL will report this to the Head Teacher, DPO and Chair of Governors. Police will be notified if necessary.
- Steps will be retraced and the location visited/contacted to find out if the documentation is still on site, or if CCTV can be examined to determine the whereabouts of the data.
- Any personal data which might have been released is identified and potential consequences will be assessed & mitigated.
- DPO will support the school in recording and reviewing the breach and school procedures including actions which need to be taken to reduce the risk of this happening again.