A Place to Flourish
"I have come that they may have life, and have it to the full" (John 10:10)

Data Protection Policy (including Clear Desk Policy)

Statutory Policy

Date of review/adoption	Spring 2024
Date of next review	Spring 2025
Notes	Adapted from Schools' Choice Model Policy 2021

Signed …*C. Robertson*… Chair of Governors

Date ………05.02.2024………

Electronically signed and approved at Full Governing Board Meeting held on 05.02.24

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

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

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.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental

	• Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others and, therefore, is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

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

5.2 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 for individuals whose data the school processes, and for the ICO.

Our DPO is Schools' Choice and are contactable via data.protection@schoolschoice.org

5.3 Headteacher

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

5.4 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 in the following circumstances:
  - o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - o If they have any concerns that this policy is not being followed;
  - o If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
  - o 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 or an area without an appropriate adequacy regulation;
  - o If there has been a data breach;
  - o Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
  - o If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:
- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract;

- The data needs to be processed so that the school can **comply with a legal obligation**;

- The data needs to be processed to ensure the **vital interests** of the individual, e.g. to protect someone's life;

- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions;

- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden);

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's data retention policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;

- We need to liaise with other agencies – we will seek consent as necessary before doing this;

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, or any location without an adequacy regulation, we will do so in accordance with data protection law.

9. Complaints

We take any complaints about our collection and use of personal information seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance by contacting the school office or Schools' Choice on data.protection@schoolschoice.org

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed

- Access to a copy of the data

- The purposes of the data processing

- The categories of personal data concerned

- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted to the DPO using the appendix contained at the end of this document. They should include:

- Name of individual

- Correspondence address

- Contact number and email address

- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

10.2 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.

10.3 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.

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

- Prevent processing that is likely to cause damage or distress

- Be notified of a data breach in certain circumstances

- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. 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.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school brochures, newsletters, on Class Dojo, Tapestry etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns etc.

- 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.

When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);

- Completing data privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);

- Integrating data protection into internal documents including this policy, any related policies and privacy notices;

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;

- Maintaining records of our processing activities, including:

    o For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);

    o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. Data security and storage of records

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

In particular:

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

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access (cover sheets will be used if necessary);

- Where personal information needs to be taken off site, staff must ensure that they store it appropriately and in a secure manner;

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment;

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. We will also maintain a disposal register to keep a record of any data which has been securely destroyed.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

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

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

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;

- Safeguarding information being made available to an unauthorised person;

- The theft of a school laptop containing non-encrypted personal data about pupils.

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Bring Your Own Device Policy

The school recognises that many employees will have their own personal mobile devices (such as smartphones and tablets) which they could use for school purposes and also that there can be benefits for both the school and staff in permitting such use. However, the use of personal mobile devices for school purposes can give rise to an increased risk in terms of the security of the school's IT networks and communications systems, the protection of confidential or otherwise sensitive information and compliance with legal obligations, such as data protection requirements.

With the prior permission of their manager, employees may use a personal mobile device for school purposes, provided always that they adhere to the terms of this policy. However, employees are not required to use their personal mobile device for school purposes if they do not wish to do so.

Before using a device under this policy for the first time, employees must erase all information and software related to any previous employment.

18.1 Scope and purpose of the policy

This policy applies to all employees who use a personal mobile device for school purposes. It applies to use of the device both during and outside their normal working hours and whether or not their use of the device takes place at the school. This policy applies to all devices which are used to access the school's IT resources and communications systems, which may include smartphones, mobile phones, tablets, laptops etc.

When staff access the school's systems, they may be able to access data about the school and our pupils, parents, contractors or suppliers, including information which is confidential or otherwise sensitive. When they access the school's systems using a device, the school is also exposed to a number of risks, including from the loss or theft of the device (which could result in unauthorised access to the school's systems or data), the threat of malware (such as viruses, spyware or other threats that could be introduced via a device) and the loss, wrongful disclosure or unauthorised alteration or deletion of school data (which could expose the school to the risk of non-compliance with legal obligations relating to confidentiality, data protection and privacy).

The purpose of this policy is to protect the school's systems and data and to prevent school data from being deliberately or accidentally lost, disclosed, deleted or altered, while enabling employees to access the school's systems using a device.

18.2 Connecting devices to the school's systems

Connectivity of all devices is managed by the IT Technician, who must approve each device as providing an appropriate level of security before it can be connected to the school's systems or network. The IT Technician has the absolute discretion to approve or reject a device and the school reserves the right to refuse or revoke permission for a particular device to connect with its systems, for example, where a device is being, or may be, used in a way that puts, or could put, the school and its employees, pupils, parents, systems or data at risk or that may otherwise breach this policy. In order to access the school's systems, it may be necessary for the IT Technician to install software applications on the device. If any such software is removed, access to the school's systems will be disabled.

The school has the absolute right to determine what types of data can be processed on a device and what may not and staff will be advised of any types of data that is restricted or prohibited.

Where a device which is connected to the school's systems develops a technical problem, fault or failure, the IT Technician will provide initial technical support to assist in determining if the issue with the device is software or hardware related. If the issue is hardware related, or relates to software which staff have installed, then they will be responsible for resolving it, including any repairs, maintenance or replacements costs and services. If it relates to software the school has provided, then it will provide any necessary support.

18.3 Device monitoring

The content of the school's systems and data is the property of the school. All data, information and communications, including but not limited to email, telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received from, or stored or recorded on a device during the course of the school's business or on the school's behalf, is the school's property, regardless of who owns the device.

The school reserves the right (remotely or otherwise) to inspect, monitor, intercept, review, disclose, remove or destroy all content on the device that has been created for or on behalf of the school and to access applications used on it for this purpose. This includes the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, printing, removal, destruction or deletion of transactions, messages, communications, posts, logins, recordings and other uses of the device. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, employees should have no expectation of privacy in any personal data on the device.

Employees are advised not to use the school's systems for communications of a sensitive or confidential nature because it is not guaranteed to be private.

The purposes for such monitoring are:

- to promote productivity and efficiency;
- to ensure the security of the school's systems and their effective operation;
- to prevent misuse of the device and protect school data;
- to ensure there is no unauthorised use of the school's time or systems;
- to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment;

- to ensure that employees do not used the school's facilities or systems for any unlawful purpose or activities that may damage the school's reputation;
- to ensure there is no breach of confidentiality or data protection.

The school may also store copies of any content for a period of time after it is created and may delete such copies from time to time without notice.

By agreeing to use a personal mobile device for school purposes, staff confirm their agreement to such inspection or monitoring, and to the school's right to copy, erase or remotely wipe the entire device, including any personal data stored on the device. Although the school does not intend to wipe personal data, it may not be possible to distinguish all such information from school data. Staff should, therefore, regularly backup any personal data contained on the device.

Staff also agree that they use the device at their own risk and that the school will not be responsible for any loss, damage or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of the device, its software or its functionality.

Staff must cooperate with the school to enable such inspection or monitoring, including providing any passwords or pin numbers necessary to access the device or relevant applications.

The school shall use reasonable endeavours not to access, copy or use any personal data held on the device, unless absolutely necessary. If such copying occurs inadvertently, the school will delete such personal data as soon as it comes to its attention.

18.4 Security requirements

Staff must:

- at all times, use their best efforts to physically secure the device against loss, theft or use by persons who have not been authorised to use the device. Staff must secure the device whether or not it is in use and whether or not it is their current possession. This includes passwords, encryption technologies and physical control of the device;
- install any anti-virus or anti-malware software at the school's request before connecting to its systems and consent to the school's procedures to manage the device and secure its data, including providing the school with any necessary passwords;
- protect the device with a pin number or strong password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, they must change it immediately;
- ensure that access to the device is denied if an incorrect pin number or password is input too many times and ensure that the device automatically locks if inactive for a period of time;
- maintain the device's original operating and security system and settings, and keep it current with security patches and updates;
- prohibit use of the device by anyone not authorised by the school, including family and friends;
- not download and install untrusted or unverified software or applications unless explicitly authorised by the school - if in doubt, contact the school's IT Technician;

- not download or transfer any restricted or prohibited types of school data to the device, for example, via email attachments, or store any such restricted or prohibited types of school data on the device unless they have been specifically authorised to do so, and they must immediately erase any such information that is inadvertently downloaded to the device;
- not backup the device locally or to cloud-based storage applications where that might result in the backup or storage of school data and any such backups inadvertently created must be deleted immediately;
- where they are permitted to store school data on the device, ensure that it is encrypted using appropriate encryption technologies approved by the IT Technician.

If the school discovers, or reasonably suspects, that there has been a breach of this policy, including any of the security requirements listed above, it shall immediately remove access to its systems and, where appropriate, remove any school data from the device.

In the event of a lost or stolen device, or where staff believe that a device may have been accessed by an unauthorised person or otherwise compromised, they must report the incident to the Headteacher immediately. Appropriate steps will be taken to ensure that school data on, or accessible from, the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work email account, even if such e-mails are personal in nature). Although the school does not intend to wipe personal data, it may not be possible to distinguish all such information from school data.

On termination of employment, on or before an employee's last day of employment by the school, all school data (including work emails), and any software applications provided by the school, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to the IT Technician for wiping and software removal. Staff must provide all necessary cooperation and assistance to the IT Technician in relation to this process. The same process will apply if an employee intends to sell the device or to return it to the manufacturer or take it to a third party for repair or replacement.

18.5 Costs

Staff must pay for their own device costs under this policy including, but not limited to, voice and data usage charges and any purchase, repair or replacement costs. Staff acknowledge that they are responsible for all costs associated with the device and that their school usage of the device may increase their voice and data usage charges.

18.6 Disciplinary action

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the school's disciplinary procedure. Breach of this policy may also lead to the school revoking an employee's access to its systems, whether through a device or otherwise.

Employees are required to cooperate with any investigation into suspected breach, which may involve providing the school with access to the device and any relevant passwords and login details.

19. Clear Desk Policy

The school operates a clear desk policy for all employees for the following reasons:

- it reduces the threat of a security breach as passwords and other confidential information are locked away or otherwise securely stored;
- it ensures compliance with data protection requirements because personal data must be held securely at all times;
- it protects employees' health and safety by reducing the risk of workplace accidents;
- it reduces the risk of damage or destruction to information in the event of a disaster such as a fire or flood etc;
- it portrays a professional image to our parents, visitors and suppliers when they visit the school's premises.

19.1 Procedure

At the end of the working day, or when staff leave the workplace for an extended period during the day, they must tidy their workplace and tidy away all school-related paperwork and files into a desk drawer, filing cabinet or cupboard in an efficient and organised manner. These should then be locked overnight where locking facilities are available. Confidential information or information containing personal data must always be securely stored. If staff are unsure of the information's sensitivity, they should either ask the Headteacher or lock it away securely.

Staff should put any paperwork that they no longer need in a rubbish/recycling bin on a daily basis. They should use the school's shredding facilities or confidential waste bags where the information in the paperwork is confidential. Any unwanted paperwork that contains personal data or sensitive information should be shredded. Paperwork that is no longer needed should be acted upon and then appropriately filed.

This policy includes removable storage media which may contain files downloaded from a computer, such as memory sticks, portable hard drives and CDs. Media of this type must also be cleared from the workplace before staff go home.

Additionally, this policy is designed to reduce the amount of paper that the school uses, which in turn reduces the amount of printing costs and filing space needed. Staff should not print out hard copies of emails or documents just to read them, unless this is really necessary. All information stored on the school's computer and email systems are backed-up, so staff will not lose the information unless they have specifically deleted it.

When printing out information, it should be cleared from printers immediately, particularly if the information is confidential or contains personal data. Scanned documents should also be deleted from the relevant scans folder on the school's network, as soon as possible. Nothing should be left lying on printers or photocopiers at the end of the day.

It is each employee's personal responsibility to adhere to this policy. If an employee fails to comply with the above rules, it will be dealt with in accordance with the school's disciplinary procedure.

20. Governor and school staff use of email

The school provides email and internet access to authorised users. The use of email within a school is an essential means of communication for staff, governors and students. In the context of school, emails should not be considered private and individuals should assume that anything they write or email could become public.

The purpose of this policy is to outline the procedure and protocols to be used when emailing and this policy must be adhered to by all authorised users.

20.1 Email accounts

The school gives all staff and governors their own email account as a work-based tool. This school email account should be the account that is used for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal contact information being revealed.

For the safety and security of users and recipients, all mail is filtered and logged. If necessary, email histories can be traced.

The following rules will apply:

- Under no circumstances should staff or governors contact students, parents or conduct any school business using any personal email addresses;
- It is the responsibility of each account holder to keep their password/s secure;
- All external emails, including those to parents, should be constructed in the same way as a formal letter;
- If any issues/complaints are involved, then staff sending emails to parents, external organisations, or students are advised to copy in the Headteacher and other relevant individuals;
- The school requires a standard disclaimer to be attached to all email correspondence, clarifying that any views expressed are not necessarily those of the school. Please note that this disclaimer is automatically added to emails sent externally;
- All emails should be written and checked carefully before sending;
- Emails created or received as part of an employee's school job will be subject to disclosure in response to a request for information under the Freedom of Information Act or a Subject Access Request in certain circumstances.

Staff are expected to manage their staff email account in an effective way as follows:

- Delete all emails of short-term value;
- Organise email into folders and carry out frequent house-keeping on all folders and archives;
- However, wherever staff access their school email (whether directly, through webmail when away from school or on non-school hardware) all the school ICT, online safety, acceptable use and email policies apply.

Staff must immediately inform the Headteacher if they receive an offensive or suspicious email and any suspicious emails should be reported to the IT Technician and should not be opened.

20.2 Sending emails

The following rules apply:

- When composing a message to a parent or non-staff member, staff should always use formal language, as if they were writing a letter on headed paper;
- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, staff should refer to the section below 'Emailing personal, sensitive, confidential or classified information';
- Staff should use their own school email account so that they are clearly identified as the originator of a message;
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate;
- Do not send whole school emails unless essential for school business;
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

20.3 Receiving emails

The following rules apply:

- Check emails regularly;
- If appropriate, staff should activate their 'out-of-office' notification when away for extended periods, e.g. school holiday periods;
- Never open attachments from an untrusted source. If unsure, always consult the IT Technician first;
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder;
- The setting to automatically forward and/or delete of emails is not allowed.

20.4 Emailing personal, sensitive, confidential or classified information

Assess whether the information can be transmitted by other secure means before using email. Emailing confidential data without the use of encryption is strictly prohibited. Users should ensure that they have read and are aware of the school's data protection policy.

Where the conclusion is that school email must be used to transmit such data, then staff should exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information;
- Verify (preferably by phoning) the details of a requestor, if unknown, before responding to email requests for information;
- Do not copy or forward the email to any more recipients than is absolutely necessary;
- Do not send the information to any person whose details staff have been unable to separately verify;
- Send the information as an encrypted/password protected document attached to an email. If staff are unsure as to how to complete this, please speak to the IT Technician;
- Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone;

- Do not identify such information in the subject line of any email;
- Request confirmation of safe receipt;
- When sending an email containing personal or sensitive data, the name of the individual is not to be included in the subject line and the document containing the information must be encrypted;
- To provide additional security, staff need to put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full governing board. If there are any changes to the legislation prior to the review date, it will be amended as and when it is necessary to do so.

22. Links with other policies

This document is linked to our:

- Freedom of Information Policy

- Staff & Volunteer Acceptable Use of Technology Policies

- Staff & Volunteer Code of Conducts

- Online Safety Policy

Appendix 1: Personal data breach procedure

This procedure is based on <u>guidance on personal data breaches</u> produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the 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:

    o Lost

    o Stolen

    o Destroyed

    o Altered

    o Disclosed or made available where it should not have been

    o Made available to unauthorised people.

- 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:

    o Loss of control over their data

    o Discrimination

    o Identify theft or fraud

    o Financial loss

    o Unauthorised reversal of pseudonymisation (for example, key-coding)

    o Damage to reputation

    o Loss of confidentiality

    o 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 and the school 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 a lockable filing cabinet in the Headteacher's office.

- Where the ICO must be notified, the DPO will do this via the <u>'report a breach' page of the ICO website</u> within 72 hours. As required, the DPO will set out:

    o 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

    o 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, all individuals whose personal data has been breached should be promptly informed in writing. 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 work with the school to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- Both the DPO and the school 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 a lockable filing cabinet in the Headteacher's office.

- The DPO and the school will review what happened and how it can be stopped from happening again.

Actions to minimise the impact of data breaches

We 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. We 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 attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the IT Technician will try to recall it.

- In any cases where the recall is unsuccessful, the DPO will advise that contact is made with 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.

- We will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

Other types of breach that you might want to consider could include:

Details of pupil premium interventions for named children being published on the school website

- The information will be removed immediately from the website.

- The parents of the named children will be contacted by letter. The letter will contain a full apology and an explanation of how the breach happened and details of the steps being taken to rectify the situation.

- The DPO will be contacted for advice and this advice will be followed fully.

- Records will be kept of the process and outcome and these will be stored in a lockable filing cabinet in the Headteacher's office.

Non-anonymised pupil exam results or staff pay information being shared with governors

- The information will be removed immediately from Governor Hub.

- Governors will be contacted and requested to remove the information from their devices etc.

- The DPO will be contacted for advice and this advice will be followed fully.

- Records will be kept of the process and outcome and these will be stored in a lockable filing cabinet in the Headteacher's office.

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- The police will be contacted to report the incident.

- The IT Technician will be contacted for support and advice.

- The DPO will be contacted for advice and this advice will be followed fully.

- Records will be kept of the process and outcome and these will be stored in a lockable filing cabinet in the Headteacher's office.

The school's cashless payment provider being hacked and parents' financial details stolen

- The police and payment provider will be contacted to report the incident.

- The IT Technician will be contacted for support and advice.

- The DPO will be contacted for advice and this advice will be followed fully.

- Records will be kept of the process and outcome and these will be stored in a lockable filing cabinet in the Headteacher's office.

Appendix 2: Checklist for Subject Access Requests

Step/Area to Consider	Complete (if relevant) Y/N	Notes
How was the request received? (e.g. using a template form, by email, over the phone etc.)		
Is the request a subject access request for some/all personal data (and/or information about how it is used) or a routine enquiry to the school (for which a different procedure may apply)?		
Is the scope of the request clear, or is any additional information required to locate the information requested and to deal with the request? *If there is any doubt as to the status of the request or the scope of this, you may need to clarify the position with the individual.*		
Has a record been made of the date on which a request was made and when the response is due?		
Has the identity of the requester been verified?		
Has receipt been acknowledged?		
Does the school hold personal data about the requester? If not, has the requester been informed?		
Where is the personal data held? (i.e. electronic records, paper filing systems, emails etc.)		
Have all relevant managers/team leaders been communicated to that they will need to help find this data?		
Have all appropriate locations been searched? What search terms were used? (i.e. to locate emails in an inbox).		
Is any of the information which is the subject of the request due to be changed or deleted between the date of the request and the provision of the information? Have you sought to retrieve such information prior to deletion (where possible) and without undue delay?		
Is any third-party personal data included within the request? If so, has this been assessed in regard to whether such information may be disclosed? *In this instance you should take into account any express refusal of consent to disclose this information or any duty of confidentiality owed to the third party in question.*		
Have all relevant exemptions been considered? *(if applicable)*		
Have the reasons for the application of exemptions been documented, including the basis for any refusal to release third-party data? Have exemptions been applied consistently?		
Does the application of exemptions involve the redaction or extraction of any information? If so, has this been applied appropriately?		

Does the information being disclosed include any codes, acronyms or complex language which may require explanation? Have steps been taken to ensure that the information that is being disclosed is concise and clear?		
In what format will the requested information be provided? If the request was received electronically, is this being provided electronically? Is the information sufficiently secure in transmission?		
Does the covering letter include information about the processing? (e.g. purposes, disclosures, source etc.)		
Has the response been reviewed internally in accordance with applicable procedures before being sent to the individual?		
Has the register of subject access record been updated?		

Appendix 3: Data Classification

Classification	Description of Information Types
Green	No Impact - information formally made public by school or information which would have no impact on privacy or school reputation if it was to be put into the public domain by any other means.
Amber	Strictly internal or agreed partners - school information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - this could also include names, addresses and pupil numbers that pose little or no risk to privacy.
Red/Official-Sensitive	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender or sexuality.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families.
	Employee & partner personal data - personal data on employees of the school and its partners. This includes details about ethnicity, gender or sexuality.
	Safeguarding information
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality.
	School information which would have a significant impact on the reputation or business of the school if it was seen by a non-intended recipient because of commercial, legal, fraud, investigatory or other areas where confidentiality is necessary.

Appendix 4: Template Confidentiality Agreement

I, the undersigned, hereby agree that I will at all times, whether or not in the employment of this school and except where such information is in the public domain:

- maintain the strictest confidentiality with regard to the affairs of the school and its pupils, parents, suppliers and employees, except to the extent that I may be authorised to disclose them by the governing board, a court of law, any authorised or enforcement agency (such as the police) or by public interest disclosure legislation;
- refrain from revealing or using confidential information and/or data for personal gain.

I undertake to familiarise myself with the data protection procedures set down by the school as a result of the UK General Data Protection Regulation and understand that the school is obliged as a consequence to view any breach of these procedures as a serious matter of discipline.

I understand that any breach of this agreement could result in the school's sensitive and confidential data being disclosed and any such conduct on my part may render me liable to summary dismissal under the disciplinary procedure.

Name: _____

Signature: _____

Date: _____

Appendix 5: Data Breach Incident Form

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against loss, destruction of or damage to personal data. A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

As soon as you are aware of a data breach, you must notify the Schools' Choice Data Protection Officer with immediate effect.

Once you have notified the DPO at Schools' Choice, this form should be completed and returned to data.protection@schoolschoice.org

Information Management Leads

Lead	Contact Information
[Data Protection Lead]	
[Data Protection Officer (DPO), if different from above]	

1.	Name of the person who identified the breach	
2.	Job title and contact details	
3.	Establishment Name	
4.	When did the breach happen?	Date: Time:
5.	When did you discover the breach?	Date: Time:
6.	If there has been a delay in reporting this breach, please explain why	
7.	How did you find out about the breach?	
8.	Tell us in as much detail as	

	you can about what happened, what went wrong and how it happened.	
9.	What preventative measures did you have in place?	
10.	Is this a breach of data by a supplier or partner organisation? (If the breach has been notified to you by a supplier or a partner organisation who you share your data with, name of the supplier/partner, date notified, contact should be completed)	The breach originated in your establishment: **Yes/No** We have been notified of the breach by a supplier/ partner organisation. **Name:** **Name Contact:** **Date Notified:** **[Insert Link to the saved notification]**
11.	Was the breach caused by a cyber incident (e.g. phishing)	**If yes please also complete section "Cyber incidents only"**
12.	Who has been notified of the breach to date? (e.g. Headteacher, DPO, ICO, parents, teachers, governors etc.)	
13.	Have you told, or are you planning to tell any other organisations about the breach? (e.g. the police, other regulators or supervisory authorities, in case we need to make contact with other agencies)	
14.	Have you told data subjects about the breach?	
15.	Number of personal data records concerned?	
16.	How many data subjects could be affected?	
17.	Categories of personal data Please highlight those that are relevant.	Data revealing racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership

		Sex life data
		Sexual orientation data
		Gender reassignment data
		Health data
		Basic personal identifiers, e.g. name, contact details
		Identification data, e.g. usernames, passwords
		Economic and financial data, e.g. credit card numbers, bank details
		Official documents, e.g. driving licences
		Location data
		Genetic or biometric data
		Criminal convictions, offences
		Not yet known
		Other (please give details below)
18.	Categories of data subjects	Employees
		Pupils
		Parents or prospective parents
		Children
		Vulnerable adults
		Not yet known
		Other (please give details below)
19.	Potential Consequences of the breach	
20.	Is the personal data breach likely to result in a high risk to data subjects?	
21.	If the data has been lost or stolen, were there any protections in place such as encryption?	
22.	Had the staff member involved in this breach received data protection training in the last two years?	

23.	Describe the actions you have taken, or propose to take, as a result of the breach.	
24.	Have you taken actions to contain the breach? Please describe these remedial actions.	
25.	Please outline any steps you are taking to prevent a recurrence and when you expect they will be completed.	
26.	What is the likelihood that data subjects will experience significant consequences as a result of the breach? Please highlight. i.e. Risk to physical safety as a result of the breach Risk of the data being used to discriminate against an individual Risk to the reputation of any individual being impacted by the breach Risk of financial loss through identity theft	**The ICO will need to be notified within 72 hours of all data breaches where a risk to individual's rights and freedom exists.** Very likely Likely Neutral (neither likely nor unlikely) Unlikely Very unlikely Not yet known Please describe any possible impact on data subjects:
27.	Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	
28.	Further comments.	

Cyber Incidents only:

1.	Has the confidentiality, integrity	Yes

		No
	and/or availability of your information systems been affected?	Don't know
		If you answered yes, please specify:
		Confidentiality
		Integrity
		Availability
2.	Impact on your organisation Please highlight	**High** – You have lost the ability to provide all critical services to all users **Medium** – You have lost the ability to provide a critical service to some users **Low** – There is no loss of efficiency, or a low loss efficiency, and you can still provide all critical services to all users **Not yet known**
3.	Recovery time	Regular – you can predict your recovery time with existing resources Supplemented – you can predict your recovery time with additional resources Extended – you cannot predict your recovery time and need extra resources Not recoverable – recovery from the incident is not possible, e.g. back-ups cannot be restored Complete – recovery is complete Not yet known

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

To be completed by the DPO

Date received and logged:

Does this represent a 'High Risk' to the rights and freedoms of those impacted individuals? If yes, details of the communication plan:

Future mitigating actions identified:

What type of data breach is it?

A **Confidentiality Breach** has occurred if the data was unauthorised or accidentally disclosed.

An **Availability Breach** has occurred if the data was unauthorised or accidentally lost.

An **Integrity Breach** has occurred if the data was unauthorised or accidentally altered.

Date ICO notified:

Further comments:

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

Appendix 6: Data Privacy Impact Assessment

It's currently good practice to carry out a privacy impact assessment when your school is considering using data in new ways, or implementing new technology.

Under the UK GDPR, they should be carried for all new projects such as implementation of the new processes or systems where any of the answers to the questions on the next page are a 'yes'.

All areas where the processing is identified as high risk should have a Data Privacy Impact Assessment and you therefore may complete this as part of your preparations for compliance with the new regulation.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals;
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences;
- Large-scale, systematic monitoring of public areas (such as CCTV).

For example, you might do this where you've considered implementing a new web monitoring system in the classroom or sharing data with a local troubled family's initiative.

A DPIA should be reviewed regularly and remain a live document and, if a data breach has occurred in an area identified as "high risk", the original DPIA should be reviewed and updated.

Where it isn't clear whether a DPIA is required, we recommend completing one, as it is a useful tool to help comply with data protection law.

A DPIA should be carried out prior to the data processing and the data controller:

- Is responsible for ensuring that the DPIA is carried out, although someone else inside or outside the school can do it;
- Must seek the advice of the data protection officer. This advice, and the decisions taken by the controller, should be documented within the DPIA;
- Must seek the views of data subjects or their representatives, where appropriate.

While there is no legal requirement to publish a DPIA, the controller can choose to do so.

Question	Yes/No
Will individuals provide information about themselves? Will this be stored electronically? Will this be stored manually?	
What is the reason for holding this data?	
Will you make decisions or take actions form this data? Consider and detail some of the impacts should this data be incorrect, lost or stolen.	
Will the project involve the collection of new information that you have not previously held?	
Will the information be shared or disclosed to individuals who do not currently have access to this? **Note: An example of this is where you buy in a service such as milk for the children and you share details with the provider.**	
Are you implementing new technology which might be perceived as being privacy intrusive? Biometrics or facial recognition? **Note: An example of this is the implementation of a fingerprint payment system. The implementation of CCTV in school would be another.**	
Does the information being collected contain. Health Records, Criminal Records for example or any other information which is considered private?	
Will you to contact individuals in ways which they may find intrusive?	

1. Explain why you are collecting the data.
2. Link any project documents. (If you are implementing a new system, the specification etc.)
3. Explain why you think this is "high risk".

The Need for the DPIA

Data Flows

Who are we consulting with to identify privacy risks?

Stakeholders

Where/who will capture the data?

Where will the data be stored?

How long will it be kept?

How will it be kept up to date/reviewed?

How will it be destroyed?

e.g. highly sensitive data posted to the wrong location as address details not up to date.

Identify the Privacy and Related Risks (What are the potential problems?)

Privacy Issue	Risk to Individuals	Risk Level
e.g. highly sensitive data posted to the wrong location as address details not up to date.	e.g. medical records included in the data which could impact the way the individual is treated by others.	

Identify the Privacy Solutions (What can we do about it?)

Risk	Solution(s)	Result *(Is the risk reduced, eliminated, acceptable?)*	Evaluation *(Is the final impact after implementing, justified, compliant and proportionate to risk?) i.e. reduction of risk to acceptable level.*

Sign Off and Record the DPIA Outcomes

Risk	Approved Solution	Approved By	Review Date

Action Plan

Any actions should be added to the General Data Protection Compliance Action Plan and any significant risks should be added to the school's risk register.

If produced for project, then individual actions can be added below:

Action to be taken	Date for completion of actions	Responsibility for action

Appendix 7: Data Sharing Decision Form

Name of requesting organisation:	
Name and position of person requesting data:	
Data requested:	
Purpose:	
Decision:	
Data supplied:	
Decision taken by: *(name and position)*	
Date of disclosure:	
Any specific arrangements: *(re. retention/deletion of data)*	
Reason(s) for disclosure or non-disclosure:	
Date request responded to:	
Signed:	
Dated:	

Appendix 8: Incident Grading Document

Incident grading 1 = Negligible
Any type of incident formally recorded, or something worthy of investigation but turns out to be a "false positive", "near miss" or loss of equipment where there is a remote chance of the data being readable, which has negligible impact on privacy or school. *Reporting of such incidents is still valuable and should be used as part of ongoing information security risk assessment.*

Incident grading 2 = Minor	
Confidentiality	Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no health or safety impacts (e.g. just name, address, pupil number at amber level)
Integrity	Confirmed or likely issues relating to integrity of information on <10 staff or pupils such as confused identities, out of date information or records misplaced which causes localised inconvenience or delays.
Availability	Some localised and short-lived loss of availability, such as through a temporary systems failure, which leads to the disruption of non-critical teams/areas.

Incident grading 3 = Moderate	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals OR any breach of "OFFICIAL- SENSITIVE" information at red level. Likely local media interest and adverse publicity.
Integrity	Issues relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other implications.
Availability	Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of local team business continuity plans. This may be either a short disruption to a very critical team/area or a longer disruption to a group of less critical teams/areas.

Incident grading 4 = Major	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals OR loss of any sensitive personal data at red level which is highly likely to affect the health or safety of one or more individuals OR any privacy breach which, because of the high-profile nature of the person(s) affected or other circumstances, is likely to lead to national media attention and cause significant reputational damage.
Integrity	An integrity issue which means data relating to 100+ staff or pupils is in effect no longer usable or understandable (and cannot be rectified) and is likely to impact health, and safety or key teams/areas/the school.
Availability	Sustained loss of availability of information which has serious impact on the delivery of a number of critical areas, resulting in business continuity plans being invoked for at least one business area.

Incident grading 5 = Extreme	
Confidentiality	Loss of data or privacy breach relating at large scale (i.e. 100,000+ persons or complete datasets); likely national/international media adverse publicity, prolonged damage (for example parent trust) and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.
Integrity	Integrity problem which leads to significant amounts of data on 100,000+ persons being unreadable or unusable and does directly lead to health and safety issues or significant services issues (e.g. entire data set for pupil group corrupted beyond use that must be recreated).
Availability	Outage or other issue which leads to general failure of IT so that teams/areas which are critical to the school are not running for a prolonged period. Business Continuity Plans across school/trust are invoked.

Appendix 9: Subject Access Request Form

Name:
Telephone Number:
Email:
Address:
Employee Payroll Number *(if relevant)***:**
By completing this form, you are making a request under the UK General Data Protection Regulation (UK GDPR) for information held about you by the school that you are eligible to receive.
Required information (and any relevant dates): *Example: Emails between "A" and "B" from 1 May 2017 to 6 September 2017.*
By signing below, you indicate that you are the individual named above. The school cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to *insert name of individual/DPO*. Please allow 1 calendar month for a reply.
Data Subject's Signature:
Date: