Wellington School

Honesty Community Excellence Fairness Endeavour

Data Protection Policy

Updated: September 2021

Review Date: September 2023

Wellington School

Policy Title	*Data Protection Policy*

Summary of Contents

The Policy outlines procedures for data protection.

Date of Update	September 2021
Review Date	September 2023
Status	Statutory
Member of SLT Responsible	S Beeley

Contents

1. Aims and Introduction

Our School aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the UK – General Data Protection Regulation (UK-GDPR) and Data Protection Act 2018.

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

Everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

School's hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for our School to use technology to benefit learners.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the UK-GDPR. Following the UK's departure from the European Union, the Government has confirmed that the UK will continue to adopt the legislation and principals of the GDPR for the time being, it will simply be referred to as the UK-GDPR. This policy will be reviewed and amended accordingly should any future changes occur.

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 complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified (includes contact details, class lists containing UPN, marks and grades)
Sensitive personal data	Data such as: • SEND/PP information • Racial or ethnic origin • Political opinions

	• Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our School processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our School delegates the responsibility of data controller to the Board of Governors.

The School is registered as a data controller with the Information Commissioner's Office (Registration Number: Z4838677) and renews this registration annually on 25th June.

5. Data protection principles

The UK General Data Protection Regulation (effective 1st January 2021) was enacted into UK law by the Data Protection Act 2018 is based on the following data protection principles, or rules for good data handling, that data is:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the 'accountability principle' requires the school to take responsibility for what we do with personal data and how we comply with the other principals listed above.

6. Roles and responsibilities

6.1 Overview

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.

The governing board has overall responsibility for ensuring that the School complies with its obligations under the Data Protection Act 2018.

Day-to-day responsibilities rest with the headteacher, or the Deputy Headteacher in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

The School Data Protection Officer is responsible for overseeing the personal data processing activities and advising and guiding on data protection law and practices. Our DPO is Sharon Pipe of RADCaT Ltd and is contactable via info@radcat.co.uk or 01942 590785.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the School of any changes to their personal data, such as a change of address.

6.2 Data Protection Act

In practice the act means that school must ensure:

1. We have legitimate grounds for holding the data that we process it in a way that won't have adverse effects and we're transparent about the data we collect and what we use it for.
2. We're clear about why we need the data and what we're going to use it for, that we publish a "privacy notice" explaining this, we notify the Information Commissioner's Office of the type of data we hold and any new uses of the data are fair.
3. The data we hold is sufficient for the purpose, but we hold no more than we need.
4. We take reasonable steps to ensure the data is accurate, and updated when necessary.
5. We consider how long we keep the data and delete it securely when it's no longer needed.
6. We uphold the subject's rights to:
   a. Get copies of the information we hold about them ("Subject Access Requests").
   b. Object to the processing of the data.
   c. Opt in' to any direct marketing.
   d. Object to automated decisions.
   e. Have their data corrected or erased.
   f. Potentially claim damages in the event of a breach of the Act.

7. That security and policy is in place to protect the data we hold and stop it being lost or obtained by someone outside of the organisation who shouldn't have it and that we have procedures in place should something go wrong.
8. That we ensure the data will be subject to similar regulations should it be transferred abroad.

6.3 Collecting Personal Data -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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security, or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise, or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
- We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

6.4 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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 record retention schedule.

6.5 Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including but not limited to:

- The prevention or detection of crime / 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
- The emergency services and local authorities to help in response to an emergency situation affecting pupils / staff

Any data transferred out of the United Kingdom will be done so in accordance with data protection law.

6.6 General Data Security

The accessing and appropriate use of school data is something the School takes very seriously. At this school we have an Acceptable Use Agreement which is reviewed at least annually, which all staff sign. Copies are kept on file.

ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors and suppliers who will use the School's IT Systems. Guidance documents (i.e. this Policy) are issued to all members of the School who have access to sensitive or personal data.

Personal data and Sensitive personal data must be encrypted if the material is to be removed from the school.

- The use of unencrypted media for the transfer of Personal data and Sensitive personal data is not permitted.
- At this school we use approved sites to securely transfer CTF pupil data files to other establishments.

All data is transferred internally via SIMS or as files which remain stored on the school network or approved cloud storage platform (although may be accessed via the secure Remote Desktop).

Personal data and Sensitive personal data must be kept out of sight, ideally held in a lockable room, storage area, drawer or cabinet if in an un-encrypted format (such as paper) when not in use.

- We store such material in lockable desk drawers or behind locked staffroom doors.
- Servers are locked in a secure server room managed by DBS-checked staff.
- Backups are stored securely offsite or in approved, cloud hosted storage.
- Disposal: Personal data and Sensitive personal data electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.
- We use recommended disposal firms to securely destroy drives where personal data may have been stored.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Disks are overwritten or physically destroyed prior to recycling where they may have been used for storing personal data.
- Laptops used by staff at home (loaned by the school) where used for any protected data will be encrypted.
- Domain Administrators with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by the Headteacher.

Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation and training will be provided to keep staff informed.

6.7 IT Security

The school gives relevant staff access to its Management Information System, with a unique ID and password.

- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data, outlined in this policy together with the eSafety policy and AUA.
- Staff have been issued with the relevant guidance documents and the ICT Acceptable Use Agreement.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Any portable equipment or media containing sensitive data must be encrypted. If in doubt, contact your IT Services team who can advise further.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared photocopiers (multi-function print, fax, scan and copiers) are used.
- Anyone expecting a confidential/sensitive fax should have warned the sender to notify before it is sent.
- Personal data (e.g. class lists) should not be included in internal email attachments since these attachments will usually be downloaded in order to be read – instead the contents should be included in the body of the email which is only resident on the viewer's machine for as long as the email is displayed.
- Personal data and Sensitive personal data should not be emailed or otherwise transmitted unencrypted unless this is unavoidable.

- When conducting due diligence studies on potential contractors or suppliers, consideration should be made of how the contractor will act as a potential data processor (e.g. how will data be transferred or received?).
- Personal data and Sensitive personal data should not be downloaded onto personal computers.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Ensure hard copies of data are securely stored and disposed of after use

It is easy to encrypt information within Microsoft Office (simply click "Protect Document" from within the file menu in Office 2016) – encryption passwords should be shared by a means other than that by which the document is being transmitted (e.g. for emailed files, phone the recipient to confirm the password). Use a new "one time" password for sharing such information – not one you use to log in to other systems!

You are strongly advised to keep an unencrypted copy of such files should it be necessary to access the file in future – files encrypted in this manner *cannot* be accessed without the password *by design*.

6.8 Bring Your Own Device (BYOD)

Many staff have their own device which they wish to use for school purposes (e.g. reading email, checking calendars and potentially storing personal data about students). **Even though the device may belong to a member of staff, the data remains the responsibility of the School as Data Controller**.
If staff wish to use their own mobile device to process (e.g. record, modify or simply store) any personal data, these devices *must* comply with the following rules:

- The device must be protected by a passcode of at least 4 digits.
- The device must be set to lock automatically after no more than thirty minutes of inactivity.
- No personal data relating to members of the School should be backed up or stored in unapproved "cloud" services such as Drop Box, iTunes etc.
- Devices must not be "rooted," "jailbroken," or contain Apps which have been installed from untrusted sources.
- The device must be connected to School email via Exchange/ActiveSync to enable remote wipe.
- The device owner must undertake to notify IT Services immediately that the device is suspected lost or stolen so a remote wipe can be initiated.

Staff should be clear about the implications of the last two points. Should a device be lost or stolen, they are under obligation to notify IT Services who will immediately send a remote wipe request to the device. This will have the effect of erasing the entire device and any installed removable media cards. Should the device be found subsequently, it will not be possible to restore any data. It is the responsibility of staff to ensure their own data (photos, contacts, etc.) are backed up.

Devices owned by staff are subject to AUA in the eSafety policy for the duration they remain connected to the School network or on School sites.

6.9 School Owned Devices

If the school has a Mobile Device Management (MDM, e.g. Meraki) system in place, then all school owned hardware should have this system deployed in order to simplify management and enhance security.

6.10 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the School's Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher.

It is the responsibility of all staff to remain vigilant against the loss or unfair processing of data.

6.11 Passwords

- Always use your own personal passwords to access computer-based services – do not use the accounts of others.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff must change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords on paper or in an unprotected file.
- IT Services will not ask you for your password, although it may on occasion be necessary to reset your password to a mutually agreed one. Ensure that all personal passwords that have been mutually agreed are changed once the work is complete.
- Passwords must contain a minimum of six characters and be difficult to guess.
- User ID and passwords for staff and students who have left the school are disabled once the period of employment has ended – you will not be able to access files or emails after this time.
- **Do not share your password with others.**
- **If you think your password may have been compromised or someone else has become aware of your password change your password immediately and report your concerns to IT Services.**
- **If you become aware of a security breach, please notify IT Services immediately.**

6.12 Password Security

- Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's policies on e-safety and Data Security.
- Students are not allowed to deliberately access on-line materials or files on the School network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.
- All networked workstations have an automatic screen saver (password protected) set to 15 minutes.
- However, all staff are advised to lock their workstation when leaving their PC unattended – this can be done by pressing "Windows" key and "L" at the same time on Windows machines – your password will be required to log in again.
- Do not leave computers locked when someone else may require access, particularly computers in classrooms – log out completely in this case.

6.13 Remote Access

- Some academies provide remote access functionality ("Terminal services," "Remote Desktop," "CITRIX," etc) which should always be used in preference to other means of accessing information.
- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- Never write down your password – pick a password which is easy for you to remember but hard for someone else to guess.
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from an external environment (e.g. at home).

- Do not use the remote access facility as a means to download Personal data and Sensitive personal data (including class lists).

7. 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. Please see our CCTV policy for further details.

Any enquiries about the CCTV system should be directed to Headteacher or Deputy Headteacher.

8. Action in the event of a data breach

In the event of a data breach, there are four main areas to be addressed:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

8.1 Containment and Recovery

The Headteacher should take the lead in assessing what information has been lost or otherwise compromised, and determine who needs to be notified. The Headteacher will then determine, with appropriate staff, what steps to take to contain the breach and recover the data. If appropriate, the police should be informed (e.g. theft of laptop).

8.2 Assessment of ongoing risk

An assessment needs to be made of the likely impact of the loss of data, depending on the type of data involved, the sensitivity of the data, to whom the data belongs and how much data has been lost. An assessment should also be made of any potential harm (e.g. financial, emotional) which may come to the individuals whose data has been lost, or harm to the reputation of the school.

8.3 Notification of breach

The individuals whose data has been lost should be contacted, with a view to advising them of any potential impact of the data loss. In the event of a serious loss of data it may be necessary to inform the ICO of the breach (e.g. loss of a large number of records).

8.4 Consequences of Failing to Report a Breach

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58, a sample of which are as follows:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

e) to order the controller to communicate a personal data breach to the data subject;

f) to impose a temporary or definitive limitation including a ban on processing;

NB: This list is not exhaustive

So, it's important that staff follow the breach-reporting process in place within this policy.

8.5 Evaluation and response

The cause of the breach must be investigated, and measures put in place to prevent the breach from recurring. The facts and cause of the breach will be recorded. The Data Breach: What To Do flowchart will be followed. (Appendix 1).

9. Safe use of images

9.1 Consent of adults who work at the school

Permission to use images of all staff who work at the School is sought on induction and a copy is located in the personnel file.

Should a member of staff not wish to have their photograph used on the School website they can request its removal by the IT Services team. These requests should be made in writing to the Headteacher.

9.2 Publishing student's images and work

On a student's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the School web site, or social media feeds.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Parents/carers may withdraw permission, in writing, at any time, or by other means provided by the school. This consent is considered valid after the child has left the School unless School is informed otherwise. Students' full names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published.

Where students' full names are to be published (e.g. to celebrate examination results), parents/carers will be given opportunity to opt out.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed from an up-to-date list.

9.3 Storage of Images

Images / films of children are stored on the School's network.

- CCTV is used for security purposes.
- Rights of access to this material are restricted to the staff and students within the confines of the School network, or via secure Remote Desktop connections.
- Images and videos of students recorded or stored on personal equipment (e.g. trips, mementoes of previous classes) will be in line with appropriate legislation and the Teachers' Standards.

9.4 Webcams

- Webcams in School are only ever used for specific learning purposes, e.g. monitoring hens' eggs or video conferencing.
- Misuse of the webcam by any member of the community will result in sanctions.
- Consent for publication of images is assumed to extend to use of webcams.

9.5 Video conferencing and online meetings

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of Wellington School.
- All students are supervised by a member of staff when video conferencing with end-points beyond Wellington School.
- Approval from the eSafety Coordinator is sought prior to all video conferences with end-points beyond Wellington School.
- The School conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the consent of the parents/carers of those taking part.

10. Use of Biometric Data

Any biometric information (defined as: "*personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements"*) must be stored in accordance with Data Protection legislation. However, if that information is also used for an automated biometric recognition system (e.g. fingerprint recognition for pre-payment dinner money), Schools must also comply with sections 26-28 of the Protections of Freedoms Act 2012. Page 11.

In essence, Academies must notify parents (or carers) of the intention to use biometric data, giving parents the right to opt out should they wish. Alternatives (e.g. a card payment system) must be provided for students who choose to opt out.

11. ICT Equipment including portable and mobile equipment and removable media

This section should be read in conjunction with the equivalent section in the eSafety policy.

11.1 School owned ICT equipment

- It is imperative that you save your data on a frequent basis to the school's network drive or approved cloud storage. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive or cloud storage. **No personally identifiable or sensitive data should be stored on your own equipment**.
- The safest way to ensure the safety of your data, and the security of sensitive data, is to use the Remote Desktop system provided by the school, or approved cloud storage which meets appropriate data protection requirements.
- Personal or sensitive data must not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

11.2 Portable and Mobile ICT Equipment

This section covers such items as laptops, mobile phones, tablets and removable data storage devices.

- Staff must ensure that all school data is stored on the school's network or approved cloud storage.
- **No personally identifiable or sensitive data may be stored on any unencrypted media.**

- Equipment must be kept physically secure in accordance with this policy. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Use Remote Desktop to access the school's systems where available.

11.3 Systems Access

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Any information held on school systems, hardware or used in relation to school business may be subject to The Freedom of Information Act.
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1988.

11.4 Telephone Services

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
- Be aware of Data Protection legislation when engaged in telephone conversations – do not divulge personal or sensitive information. See the Data Protection policy for further guidance.

12. Privacy Notices

12.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the School is performing. Further details of how we process your data can be found in the privacy notice on our website

12.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our School. We also, collect data from applicants for positions at our school. For further information on how we process your data please see our Staff Fair Processing Notice.

Any staff member wishing to see a copy of information about them that the School holds should contact the Headteacher.

12.3 Visitors

We process the data of any visitors entering the school site for identification purposes and to ensure safety within the school community. For further information on how we process visitor information, please see the privacy notice on the school website or upon your arrival at reception.

13. Subject access requests

Under the UK-GDPR and Data Protection Act 2018, staff, pupils and their parents have the right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax, whereupon we will respond to the request within 30 days. The school has a right to extend the response time by two months for any complex requests; a response will be provided informing the requester of the proposed extension.

Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The School will not reveal the following information in response to subject access requests:

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

14. Parental requests to see the educational record

Parents of pupils at this School do not have an automatic right to access their child's educational record. The School will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights). Where parents request exam results earlier than the release date, we will not release the information until we are able to do so following the guidance issued by the Information Commissioner.

A response containing the information or outlining reasons why the request cannot be met will be provided within 15 days.

15. Storage of records

The school will protect personal data and keep it safe from unlawful access, alteration, processing, damage or disclosure. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the School office
- 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 for School-owned equipment. Please refer to the school's Acceptable Use Policy for further information.

16. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. A log of all data disposed of will be kept by the school.

17. Training

Our 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, and we will annually refresh training with our staff on various data protection topics.

18. The UK General Data Protection Regulation

Following the UK's departure from the European Union, the government updated the data protection legislation to now refer to the GDPR as UK-GDPR which continues to run alongside the Data Protection Act 2018. This change in name took effect from 1st January 2021 and so far, no significant changes have been made, the UK will still follow the incumbent GDPR principals but will have full control over any future amendments.

19. Monitoring arrangements

The Headteacher is responsible for monitoring and reviewing this policy.

The Headteacher checks that the School complies with this policy by, among other things, reviewing School records regularly.

This document will be reviewed every 2 years or sooner should a significant update occur.

At every review, the policy will be shared with the governing board.

20. Links with other policies

This data protection policy and privacy notice is linked to:

- the freedom of information publication scheme
- records management policy
- CCTV policy
- acceptable use policy
- disciplinary policy
- whistle blowing policy
- safeguarding children policy

Appendix 1

PERSONAL DATA BREACH: WHAT TO DO

What is a data breach?

It's a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples of what a breach might involve:

- Non-anonymised data shared/published showing test results of children eligible for pupil premium
- Safeguarding information about a child being made available to unauthorised people
- The theft of a school laptop containing non-encrypted personal data about pupils

Why must you escalate a data breach?

1. If someone's personal data falls into the wrong hands it can result in serious harm to that person
2. We are legally required to investigate data breaches
3. Learning what went wrong will help us to adapt procedures and prevent further breaches.

Found or caused a data breach? Immediately notify: Stuart Beeley, Headteacher
He will inform our data protection officer, who will deal with the breach.
The DPO will . . .

Alert the Chair of Governors
Contain and minimise the impact of the breach taking all reasonable efforts, and assisted by relevant staff where necessary
Assess the potential consequences How serious are they? How likely are they to happen?

Risks to someone's rights and freedoms: is it likely? Could the breach put someone at risk of discrimination, identity theft, damage or disadvantage?

NO

YES

Report the breach to the ICO within 72 hours

Go to www.ico.org.uk/for-organisations/report-a-breach/ or call 0303 123 1113.

Provide information on:

- The nature of the breach, including where possible: the categories and approximate number of individuals concerned, the categories and approximate number of data records concerned
- The likely consequences of the breach
- The measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on those concerned

Give a point of contact – usually the DPO.

If not all details are available, report as much as possible and explain that there is a delay, the reasons why, and when you'll have further information. Submit the remaining information ASAP.

Risk to someone's rights and freedoms: is it high? How serious are the risks? How likely are they to happen?

YES

NO

Inform the affected individual(s) promptly

Do this in writing and set out: Your name and contact details; the likely consequences of the breach; the measures you have taken, or will take, to deal with the breach and mitigate any possible adverse effects on individuals

Notify any third parties who can mitigate the impact of the breach for example, the police, insurers, or banks

Review and record the breach

Discuss with the headteacher:
- What happened
- How we can stop it from happening again
- Whether a process or system regularly has minor incidents

Record:
Facts and cause; Effects; All decisions taken – including whether or not to report to the ICO/individuals affected
Action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)