Dringhouses Primary School

Information & General Data Protection Regulations (GDPR) Policy

Signature of Chair of Governors . . . . . .

Signature of Headteacher . . . . . .

Date of Adoption:	**Summer 2021**
Date of Review:	**Summer 2022**
Reviewing Committee:	**Full Governing Body**

Statutory/Non-Statutory

Annexes 2-4 are adopted from Veritau Ltd – Information Governance

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 UK data protection law.

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 General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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 with the ICO and has paid its data protection fee to the ICO, as 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 report 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.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is the Veritau Ltd and is contactable via the School Business Manager or via the contact information detailed in the Information Policy (annex 2).

5.3 School Business Manager (SBM)

The SBM 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/SBM in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

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 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.

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.

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.

8. 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 UK 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.

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 internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the SBM.

9.2 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.

9.3 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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/SBM. If staff receive such a request, they must immediately forward it to the DPO/SBM.

10. 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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the SBM.

13. 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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

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

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

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.

14. 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 protection 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - 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)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. 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 secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must ensure that steps are taken to ensure the safety of this data
- 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 that they should not reuse passwords from other sites
- 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 (see our ICT policy/policy on acceptable use)
- 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 (see section 8)

16. 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.

17. 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 appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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

18. 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.

19. Monitoring arrangements

The DPO/SBM is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Using Images Policy
- Information Policy (Annex 2)
- Acceptable Use Policy (Annex 5)
- Information Security & Incident Reporting Policy (Annex 4)
- Information Security Policy (Annex 3)
- Safeguarding Policy

Annex 1

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the School Business Manager (SBM), who will contact the data protection officer (DPO)
- The DPO and SBM will investigate the report, and determine whether a breach has occurred. To decide, the DPO/SBM will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO/SBM will alert the headteacher and the chair of governors
- The DPO/SBM will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO/SBM with this where necessary, and the DPO/SBM should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO/SBM will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO/SBM
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored by the DPO/SBM.

  The DPO/SBM and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO/SBM and headteacher will meet annually to audit GDPR practices and will review recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its safeguarding partners.

Details of Pupil Premium interventions for named children being published on a school website

- If special category data (sensitive information) is accidentally published on the school website the publication should be removed as soon as the school becomes aware of the error and the DPO/SBM informed.
- the DPO will consider whether it's appropriate to contact the relevant individuals whose details have been shared, explain that the information was published in error, and that the publication has been removed
- The DPO will carry out an internet search to check that the information has not been shared and made public elsewhere; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, r all, of its safeguarding partners.

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

- If a school laptop is stolen or hacked and contains sensitive information the user/owner must inform the DPO/SBM as soon as they become aware
- The DPO will ask the [ICT department/external IT support provider] to attempt to shut down access remotely to any attempt to access the device and erase any data possible to prevent it being shared unlawfully.
- The DPO will carry out an internet search to check that the information known to be contained on the laptop/device has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, r all, of its safeguarding partners.

Hardcopy reports sent to the wrong pupils or families

- If a report containing sensitive information is accidently sent to the wrong pupil/family the sender must inform the DPO/SBM as soon as they become aware of the error.
- the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way (retaining a copy if required as evidence)
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its safeguarding partners.

Annex 2

Information Policy

Introduction

This policy is to ensure that Dringhouses Primary School complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

Scope

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Information Security and security incident reporting will be addressed in separate policies.

Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

The school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Information Governance
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk

Veritau
Assurance Services for the Public Sector

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Head Teacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

Training

The school will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPO will be consulted in relation to training where necessary; to ensure training resources and their implementation are effective.

The school will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

Privacy notices

Dringhouses Primary School will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the school's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of the year as part of their information pack. A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any adhoc sharing of information will be done in compliance with our legislative requirements.

Data Protection Impact Assessments (DPIAs)

The school will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks

The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

Destruction of records

Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record

Third party Data Processors

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. . If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

Access to information

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to the School Business Manager, telephone 553940, e-mail admin@dringhouses.co.uk , who is responsible for:

Deciding whether the requested information is held;

- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

Each request received will be acknowledged within 5 school days. The Chair of Governors and headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information; and
- Where necessary seek guidance from previous case law in deciding where the balance lies
- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body meeting.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. Any charges will be formulated taking into account the limits set by the legislation.

We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 school days.

Requests for information under the GDPR- Subject Access Requests

Requests under this legislation should be made to the School Business Manager, telephone 553940, e-mail admin@dringhouses.co.uk.

Any member of staff/governor may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the school office and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of 30 **calendar** days.

The school can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information)(England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

Data Subject Rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to **the School Business Manager, telephone 553940, e-mail admin@dringhouses.co.uk ,** who will acknowledge the request and respond within 30 calendar days. Advice regarding such requests will be sought from our DPO.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Complaints

Complaints in relation to FOI/EIR and Subject Access will be handled through our existing procedures. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the DPO on the address provided.

Copyright

Dringhouses Primary School will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Annex 3

Information Security Policy

Introduction

The Information Security Policy outlines the School's organisational security processes and standards. The policy is based upon the sixth principle of GDPR which states that organisations must protect the personal data which it processes against unauthorised loss by implementing appropriate technical and organisational measures.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

Scope

All policies in Dringhouses Primary School's Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communication sent by post/courier or using electronic means such as email or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Published web content, for example intranet and internet
- Photographs and other digital images

Access Control

The School will maintain control over access to the personal data that it processes. These controls will differ depending on the format of the data and the status of the individual accessing the data. The School will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the School Business Manager.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be via locked filing cabinets. Access is limited to those who need access.

Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two tier authentication system will be implemented across all electronic systems. The two tiers will be user name and unique password.

Individuals will be required to change their password every 3 months and user names will be suspended when an individual leaves employment of the School.

External Access

On occasions the School will need to allow individuals, who are not employees of the school, to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another School. Head Teacher or School Business Manager is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access then access can also be authorised by the Deputy Head Teacher.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the School.

Physical Security

The School will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the School:

Alarm System

The School will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access

External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Head Teacher or School Business Manager will be responsible for authorising key distribution and will maintain a log of key holders.

Internal Access

Internal areas, which are off limits to pupils and parents, will be kept locked and only accessed through pin numbers, keys or fobs.

Visitor Control

Visitors to the School will be required to sign in on arrival and state their name, organisation, and person visiting. Visitors will be required to wear visitor badges at all times and will not be allowed to access restricted areas without employee supervision. They will sign out again as they leave.

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the School must also protect data against environmental hazards such as power loss, fire and floods.

It is accepted that these hazards may be beyond the control of School but the School will implement the following mitigating controls.

Back Ups

The School will back up their electronic data and systems every night. These backups will be kept off site by an external provider. Should the School's electronic systems be compromised by an environmental or natural hazard then the School will be able to reinstate the data from the backup with minimal disruption or loss.

Fire Doors

Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System

The School will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems Security

As well as physical security the School also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the School's ability to operate and could potentially endanger the lives of its Pupils.

The School will implement the following system security controls in order to mitigate risks to electronic systems:

Phishing Emails

In order to avoid the School's computer systems from being compromised through phishing emails employees are encouraged not to click on links that have been sent to them in emails when the source of the email is unverified. Employees will also take are when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the IT provider if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software

The School will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The School will update the firewalls and antivirus software when updates are made available and when advised to do so by the IT provider. The School will review its firewalls and anti-virus software in conjunction with the IT provider on an annual basis and decide if they are still fit for purpose.

Shared Drives

The School maintains a shared drive on its servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. The Head Teacher or School Business Manager will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the School's retention schedule.

Communications Security

The transmission of personal data is a key business need and, open to the following risks:

Sending Personal Data by post

When sending personal data, excluding special category data, by post the School will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post

When sending special category data by post the School will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data that is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email

The School will only send personal data and special category data by secure email transmission. Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

Exceptional Circumstances

In exceptional circumstances the School may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive usual transmission methods would not be considered secure or because the volume of data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then School employees will utilise the Blind Copy (BCC) function.

Remote Working

It is understood that on some occasions employees of the School will need to work at home or away from the School premises. If this is the case then the employees will adhere to the following controls:

If employees are working at home they will ensure that all reasonable measures are in place for ensuring that personal data is kept secure.

Employees must not keep personal data or School equipment unsupervised at home for extended periods of time (for example when an employee goes on holiday).

Employees must not keep personal data or School equipment in cars if unsupervised.

Private Working Area

Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use School equipment for their own personal use.

Trusted Wi-Fi Connections

Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from the School's IT Provider.

Encrypted Devices and Email Accounts

Employees will only use School issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing or creating personal data. This is because personal devices do not possess the same level of security as a School issued device.

Employees will not use Personal email accounts to access or transmit personal data. Employees must only use School issued or School authorised email accounts.

Data Removal and Return

Employees will only take personal data away from the School premises if this is required for a genuine business need. Employees will take care to limit the amount if data taken away from the premises.

Employees will ensure that all data is returned to the School premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

Annex 4

Information Security Incident Reporting Policy

Introduction

This policy has been written to inform Dringhouses School employees what to do if they discover an information security incident.

Queries about any aspect of Dringhouses Primary School's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at SchoolsDPO@veritau.co.uk

Scope

This policy applies to all Dringhouses Primary School's employees, any authorised agents working on behalf of Dringhouses Primary School including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Notification and Containment

Article 33 of the GDPR compels data controllers to report breaches of personal data, to the Information Commissioner's Officer, within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that Dringhouses Primary School has a robust system in place to manage, contain, and report such incidents.

Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Specific Point of Contact (SPOC) within 24 hours. If the SPOC is not at work at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the officer who located the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the SPOC will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE	Information security event No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN	Minimal Impact A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER	Moderate Impact Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.
RED	Serious Impact A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (Within 72 Hours)

The SIRO, in conjunction with the service manager, SPOC/, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The service manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents

The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the Council.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

Annex 5

Acceptable Use Policy

Introduction

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business functions.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in Dringhouses Primary School's Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communication sent by post/courier or using electronic means such as email or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Published web content, for example intranet and internet
- Photographs and other digital images

Email

The School provides email accounts to employees to assist with performance of their duties.

Personal Use

Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the school
- Employees understand that emails sent to and from corporate accounts are the property of the school
- Employees understand that school management may have access to their email account and any personal messages contained within
- Employees understand that the emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation

- Employees understand that the school reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network
- Use of corporate email accounts for personal use does not infringe on business functions

Inappropriate Use

The school does not permit individuals to send, forward or solicit emails that in any way may be interpreted as insulting, disruptive or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Unwelcome propositions
- Profanity, obscenity, slander or libel
- Ethnic, religious or racial slurs
- Political beliefs or commentary
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs or political beliefs

Other business Use

Users are not permitted to use emails carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not for profit organisations and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School Management.

Email Security

Users will take care to use their email accounts in accordance with the school's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources
- Use secure email transmission methods when sending personal data
- Not sign up to marketing material that could jeopardise the school's IT network
- Not send excessively large email attachments without authorisation from School Management and the School's IT provider

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. Head Teacher will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The School may monitor and review all email traffic that comes to and from individual and group email accounts.

Internet Use

The School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School
- Employees understand that School management may have access to their internet browsers and browsing history contained within
- Employees understand that the School reserves the right to suspend internet access at any time
- Use of the internet for personal use does not infringe on business functions

Inappropriate Use

The School does not permit individuals to use the internet in a way that may be interpreted as insulting, disruptive or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files
- Images, cartoons, jokes or movie files containing ethnic, religious or racial slurs
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations and private enterprises. This restriction may be lifted on a case by case basis by basis at the discretion of school management.

Internet Security

Users will take care to use the internet in accordance with the school's information security policy. In particular users will not click on un-trusted or unverified Web Pages.

Social Media Use

The School recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The School also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts

The School has a number of social media accounts across multiple platforms. Nominated employees will have access to these accounts and are permitted to post general information about the School. Authorised employees will be given the usernames and passwords which must not be disclosed to any other individual within or external to the organisation. The Head Teacher will have overall responsibility for allowing access to social media accounts.

Corporate Social Media Accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the School's information governance policies and data protection legislation.

Corporate Social Media Accounts must not be used in a way which could:

- Tarnish the reputation of the school
- Be construed as harassment or disparagement of others based on their sex, gender, race or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs or political beliefs
- Be construed as sexually explicit
- Construed as political beliefs or commentary

Personal Accounts

The school understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours
- Using corporate equipment
- To conduct corporate business
- To contact or approach clients, customers or partners of the School

Telephone Use

The School provides telephones for employees to assist with performance of their duties

Personal Use

Whilst the telephone should be used primarily for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School
- Employees understand that school management may have access to call history
- Employees understand that the school reserves the right to suspend telephone usage at any time
- Use of the telephone for personal use does not infringe on business functions

Inappropriate Use

The School does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School Management.