Carr Infant School

Confidence - Communication - Creativity

Information Policy Suite:-

- ICO
- Information
- Information Under Publication Scheme
- Security
- Security Incident Reporting
- Acceptable Use

July 2024

Approved by	Resources Committee
Previously Approved	May 2023
Date	July 2024
Review Date	July 2026

Model publication scheme

Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably

practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19.
The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

Classes of information

Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

Lists and registers.
Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the public authority.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Information Policy

Introduction

This policy is to ensure that Carr Infant and Nursery 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.

This policy is the School's main information governance policy and addresses:

- Data Protection (including rights and complaints)
- Freedom of Information
- Information Asset Management

Information security, acceptable use of systems 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:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL
schoolsDPO@veritau.co.uk
01609 532526
***Please ensure you include the name of the School in all correspondence with the DPO**

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 provide the School with adequate training resources and guidance materials. The DPO will be consulted, and will offer an adequacy opinion, if the School opts to use a third party training provider.

The School will maintain a 'training schedule' which will record when employees have completed an information governance training module and when a refresher is due to be completed.

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

Carr Infant and Nursery 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.
The School has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS).

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 shredding documents.

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 Administrator.
The School Administrator, in discussion with other relevant staff/governors, 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 Head Teacher 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. We will follow York City Council's charging regime for FOI/EIR.
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 Administrator.
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 Administrator 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 one calendar month.

The school can apply a discretionary extension of up a further two calendar months 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 calendar month 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 Administrator who will acknowledge the request and respond within one calendar month. 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

Carr Infant and Nursery 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.

General

The Governing Body of Carr Infant and Nursery School will be responsible for evaluating and reviewing this policy.

Guide to information available from Carr Infant and Nursery School under the model publication scheme

All documents can be obtained by contacting the school office: 01904 565140, carrinfants.school@york.gov.uk
Carr Infant and Nursery School, Ostman Road, York, YO26 5QA
For charges information, please see the end of this document.

Information to be published	**How the information can be obtained**
Class 1 – Who we are and what we do (Organisational information, locations and contacts) Current information only.	
Who's who in the school and staffing structure	Website or hard copy
Who's who on the governing body and the basis of their appointment	Website or hard copy
Instrument of government	Electronic copy via school office or hard copy
Contact details for the Headteacher and the governing body, via the school (named contacts where possible)	Website or hard copy
School prospectus	Electronic copy via school office or hard copy
Staffing structure	Website or hard copy
School session times and term dates	Website or hard copy
Address of school and contact details, including email address	Website or hard copy

Class 2 – What we spend and how we spend it (Financial information related to projected and actual income and expenditure, procurement, contracts and financial audit) Current and previous financial year	
Annual budget plan and financial statements	Hard copy
Capital funding	Hard copy
Financial audit reports	Hard copy
Details of expenditure items over £2000 – published annually	Hard copy
Procurement and contracts the school has entered into, or information relating to/a link to information held by an organisation which has done so on its behalf (e.g. a local authority or diocese)	Hard copy
Pay policy	Hard copy
Staff allowances and expenses that can be incurred or claimed, with totals paid to individual senior staff members by reference to categories	Hard copy
Staffing, pay and grading structure	Hard copy

Governors' allowances and a record of total payments made to individual governors	Hard copy

Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) Current information only.	
Government-supplied performance data	Hard copy
Latest Ofsted report	Website or hard copy
Post-Ofsted inspection action plan	Hard copy
Performance management policy and procedures adopted by the governing body	Hard copy
The school's future plans, e.g. consultation on change in status	Hard copy
Safeguarding and child protection policies and procedures	Website or hard copy

Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous three years.	
Admissions policy/decisions (not individual admission decisions)	Website or hard copy Admissions authority – York City Council
Agendas and minutes of meetings of the governing body and its committees *Excluding information that is properly regarded as private to the meeting*	Hard copy

Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only.	
School policies *All statutory policies, procedures and documents that the school is required to have as per Department for Education guidance.*	Website or hard copy
Records management and personal data policies *Including information security, records retention and destruction and data protection policies (including information sharing policies)*	Website or hard copy
Charging regimes and policies	Website or hard copy

Class 6 – Lists and registers Currently maintained lists and registers only (this does not included the attendance register)	
Curriculum circulars and statutory instruments	Website or hard copy
Disclosure log	Hard copy
Asset register	Hard copy

Class 7 – The services we offer (Information about the services we officer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only.	
Extra-curricular activities	Website or hard copy
Out of school clubs	Website or hard copy
School publications, leaflets, books and newsletters	Website or hard copy
Services for which the school is entitled to recover a fee, together with those fees	Website or hard copy

Schedule of charges

Description	**Basis of charge**
Photocopying/printing @ 2p per sheet (black & white)	Actual cost*
Photocopying/printing @ 2p per sheet (colour)	Actual cost*
Postage	Actual cost of Royal Mail standard 2nd class

*The actual cost incurred by the school, which may be more than 2p per sheet

Information Security Policy

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Long Marston CE Primary School's programme to comply with the new legislation it has written a new suite of Information Governance policies. The Information Security Policy outlines the School's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 27000:1 (internationally recognised information Security standard).
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 the 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,
- 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.

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 Administrator.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files, that contain personal data, will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use. Access to these keys will in most cases be restricted to the Headteacher and/or Administrator, with the exception of the pupil contact details file, which all staff need access to in case of emergency. (The pupil contact details file is kept in a locked cupboard in the school office and is only accessible by staff.)

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 usernames and unique passwords. Individuals will be required to change their password regularly and user names will be suspended either when an individual is on long term absence or when an individual leaves employment of the School.

Software and Systems Audit Logs

The School will ensure that all software and systems have inbuilt audit logs so that the School can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

Data Shielding

The School does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the School.

The School will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and any electronic files will be locked down so that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at the School may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

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. The Headteacher 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 School Administrator.

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:

Clear Desk Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

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 School Administrator 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 keys. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

Visitor Control
Visitors to the School will be required to sign in a visitor's book and state their name, organisation, car registration (if applicable) and nature of business. This may be either paper or electronic format. Visitors will be escorted throughout the School and will not be allowed to access restricted areas without employee supervision.

Visitor books will not be removed from the school office and will be kept for current financial year + six years.

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 and natural 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 holds 7 days of backup on an external hard drive. 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 destruction, providing the hard drive is undamaged.

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 systems security controls in order to mitigate risks to electronic systems:
Software Download Restrictions
Employees must request authorisation from the school's IT support provider before downloading software on to the School's IT systems. They will vet software to confirm its security certificate and ensure the software is not malicious. They will also retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

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 that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the school's IT support 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 anti-virus software when updates are made available and when advised to do so by the school's IT support provider. The School will review its firewalls and anti-virus software regularly 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. For example a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The School Administrator

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, when operated securely is a benefit to the School and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The School has implemented the following transmission security controls to mitigate these 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 which 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 email if one or more of the following conditions are met:

- Both the sending and receiving email addresses are GCSX or GCX etc (this usually applies to gov.uk email addresses).
- Using a secure email transmission portal such as Egress.

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 circumstance 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 the 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 occasion 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:

Lockable Storage
If employees are working at home they will ensure that they have lockable storage to keep personal data and School equipment safe from loss or theft.

Employees must not keep personal data or School equipment unsupervised at home for extended periods of time (for example when the 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 support 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 of 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.

Information Security
Incident Reporting Policy

Introduction

From May 2018 the UK's existing Data Protection Act was replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. This policy has been written to govern the School's management of information security incidents and data breaches.
Queries about any aspect of Carr Infant and Nursery 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 Carr Infant and Nursery School employees, any authorised agents working on behalf of Carr Infant and Nursery 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.

It 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.

Article 33 of the GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore it is vital that the School has a robust system in place to manage, contain, and report such incidents. The Information Security Incident Management Policy details how the School will handle and manage information security incidents when they arise.

Notification and Containment

In order for the School to report serious incidents to the ICO within 72 hours it is vital that it 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, the School Administrator and Headteacher within 24 hours. If the School Administrator or Headteacher are 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 individual who discovered 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 School Administrator and Headteacher will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings can be found in Appendix One of this document.

The School Administrator will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The School Administrator 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 relevant manager, School Administrator, Headteacher, 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 relevant manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents

The School Administrator and Headteacher 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.

APPENDIX ONE: SEVERITY RATINGS FOR INFORMATION SECURITY INCIDENTS

Rating	Incident Threshold	Recommended Actions
WHITE **Information Security Event**	No breach of confidentiality, integrity, or availability has taken place but there is a failure of the implemented safeguards that could lead to a breach in the future. *Examples* ▪ A post-it note containing a user name and password to a School database is found attached to a keyboard. ▪ A key safe, containing keys to filing cabinets, has been found unlocked and unsupervised.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on school register of incidents
GREEN **Minimal Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Incident has been contained within the organisation (or trusted partner organisation). The information does not contain any special category data or any data that would be considered to be sensitive. The actual or potential detriment to individuals is virtually non-existent. *Examples* ▪ An email, containing details of a service user's address or contact details, is sent to an incorrect recipient within the School. ▪ A document containing the only record of pupil's contact details have been destroyed in error.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on school register of incidents ▪ Notify SIRO ▪ Investigation report to be conducted by Information Asset Owner.
AMBER **Moderate Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left school control.	▪ Responsible officer(s) asked to re-sit Data Protection e-learning. Management to consider HR action. ▪ Consider utilising key messages/intranet to remind all staff of certain data protection best practice.

	The information does not contain special category data or data that is considered to be sensitive but may contain data that should have been confidential to the School. The incident appears to affect only a small number of individuals. The actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioner's Office. *Examples* ▪ A letter is sent to the wrong postal address and the incorrect recipient has learnt of another individual's dealings with the School. However, the letter does not contain any special category information. ▪ An email has been sent to ten parents without the BCC function being utilised which reveals all ten personal email addresses.	▪ Logged on School register of incidents ▪ Notify SIRO ▪ Investigation report to be conducted by Information Asset Owner .
RED **Serious Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left school control. The information contains special category data or data that is considered to be sensitive in nature and/or affects a large number of individuals. The incident has or is likely to infringe on the rights and freedoms of an individual and has a likely potential to cause detriment (emotional, financial, or physical damage) to individuals. *Examples* ▪ A file, containing safeguarding and health data, is left unsupervised in a vehicle which is subsequently stolen and the data has been lost to persons unknown. ▪ A spreadsheet containing the SEN information for all the School's pupils has been mistakenly sent to a member of the public.	▪ Management to consider (potentially immediate) HR action. ▪ Logged on school register of incidents ▪ Notify SIRO and Data Protection Officer ▪ Consider forming an incident strategy conference ▪ Consider reporting to the Information Commissioner's Office ▪ Consider informing affected individual(s) ▪ Consider informing the police or other law enforcement agencies.

		▪ Where appropriate the Data Protection Officer to conduct incident investigation with assistance (where and if required) from internal audit and counter fraud colleagues.

Acceptable Use Policy

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Carr Infant and Nursery School's programme to comply with the new legislation it has written a new suite of Information Governance policies.

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 Carr Infant and Nursery 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,
- 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.

Email Use

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 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.

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.

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 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, or political beliefs.

Other Business Use

Users are not permitted to use the internet 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.

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 links 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 different 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 to these accounts which must not be disclosed to any other individual within or external to the organisation. The Headteacher 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, racial 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 should not use these accounts during contact hours with pupils.

Telephone Use

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity is permitted.

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.