Version	May 18 v2 Updated Feb 19
Owner	Skelton Primary School
Approved	
Review Cycle	1 years
Next Review	May 20

Data Protection and Confidentiality Policy

Skelton Primary School offers a positive, safe learning environment for its community, in which everyone has equal and individual recognition and respect. We celebrate success and are committed to the continuous improvement and fulfilment of potential in every child.

We encourage increasing independence and self-discipline amongst the pupils. Everyone within the school has an important role to play in sharing responsibility for the development of positive behavior and attitudes.

Designated Safeguarding Lead -Andy Woolf

Deputy Safeguarding Leads- Sarah Walker

Tracy Hill, Charlotte Bonas

Safeguarding Link Governor Geoff Bland

Head Teacher Sarah Walker

Chair of Governors Emma McLeod

This policy will be kept under review in the light of legal developments and best practice

Next review: May 2020 SLT responsibility: A.Woolf

Introduction

This policy is to ensure that Skelton 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
01609 53 2526

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

Skelton 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 their school life 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 Skelton Primary School Office Manager

They will be responsible for:

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply, ad 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.

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 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 Skelton Primary School Office Manager

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 School Office Manager 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 School Office Manager 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

Skelton 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.

General

Skelton Primary School Governing Body will be responsible for evaluating and reviewing this policy.

Information Security Incident Reporting

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

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

This policy applies to all employees, any authorised agents working on behalf of Skelton 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 Skelton 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)- Mr A Woolf within 24 hours. If the SPOC is not at work at the time of the notification then it must be reported to the Headteacher 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.

Confidentiality Policy

1.0 LEGAL BACKGROUND

The Human Rights Act 1998 gives everyone the right to have 'respect for his private and family life, his home and his correspondence,' unless this is overridden: by the pupil interest, for reasons of child protection, for the protection of public safety, pupil order, health or morals or for the rights and freedoms of others.

2.0 AIMS OF THE CONFIDENTIALITY POLICY

- To provide clear guidance to all members of the school community around confidentiality.
- To encourage children to talk to a trusted adult if they are having problems.
- To ensure all adults working in school deal confidently with sensitive issues

3.0 SPECIFIC ISSUES

All Adults Working in Skelton Primary Academy aim to:

- Implement the Child Protection Policy
- Keep anything seen or heard within a school confidential to the school where appropriate
- Never give out a child's personal details over the telephone until the validity of the request has been ascertained.
- Never publicise images of pupils on the school website, in the local press or via newsletters if parents have expressly wished that they do not want their child's image to be in the public domain.
- Avoid unconditional confidentiality
- No adult should discuss an individual child's behaviour in the presence of another child.
- No adult should enter into detailed discussion about a child's behaviour or academic progress with other children or their parents.

4.0 Local Governor Meetings

Local Governors in particular those sitting on discipline committees, will not divulge details about individuals (be they staff, families or individual children) to any person outside of the meeting. Local Governors need to be mindful that from time to time issues are discussed or brought to their attention about staff and children. All such papers should be marked as confidential and should be copied onto different coloured paper. These confidential papers should be destroyed. Local Governors must observe complete confidentiality when asked to do so, especially in relation to matters concerning individual staff, children or parents/carers. Although decisions reached at local

governor meetings are normally made public through the minutes or otherwise, the discussions on which decisions are based should be confidential.

5.0 Information Held About Children

Information about children will be shared with parents/carers but only about their child. Parents/ carers will not have access to any other child's books, marks and progress grades at any time, especially at parents evening. However, parents/carers should be aware that information about their child will be shared with the receiving school, if and when they change school. All personal information about children including social services records are regarded as confidential. The Headteacher or Designated Safeguarding Lead will decide who will have access, and whether those concerned have access to all, or only selected information. Information regarding health report such as speech therapy, medical reports, SEND reports, SEND minutes of meetings, Social Care and Health Services will be made available to read within the electronic recording system (CPOMs). Senior Leaders will decide the level of access staff will have to this system.

6.0 Information Sharing With Other Professionals

Skelton Primary School applies the Government's seven golden rules when sharing information with other professionals. There are occasions in school where members of staff will need to consider whether information provided by a child or their family needs to be shared with other professionals. Skelton Primary School will always endeavour to gain consent when sharing information, though this may not always be possible.

Seven golden rules for information sharing

1. **Remember that the General Data Protection Regulations is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.
2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.
4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being**: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, accurate, timely and secure**: Ensure that the information you share is necessary for the purpose for which you are sharing

it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record of your decision and the reasons for it** – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Extract from HM Government Information Sharing: Guidance for practitioners and managers March 2015.

7.0 In The Classroom

Ground rules will be used where sensitive issues are to be addressed. E.g. Drugs Education, Sex and Relationships Education. Adults will remind children/students that some information they share in the classroom may need to be shared with other adults for their protection. If a child and his/her parent/ carer wish to highlight an issue to a peer group then this will be carried out sensitively by the class teacher/ head teacher. E.g. bereavement.

8.0 Monitoring and Review

The Designated Safeguarding Lead will monitor the effectiveness of the policy throughout the year in consultation with the governor with responsibility for child protection. This policy will be reviewed in light of new guidelines produced around the General Data Protection Regulations (2018).