Crockerne C of E Primary School

Inspirational Futures Trust

Name of Policy:	**Data Protection**
Committee:	**Safeguarding, Health and Safety, Premises and Finance**
Date Ratified:	**July 17**
Next Review:	**Dec 18**
Chair of Governors Signature:	
Headteacher Signature:	

Data Protection

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, common law duty of confidentiality, current Information Sharing Guidance and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data need to be aware of their duties and responsibilities by adhering to these guidelines. Information Governance refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and future regulatory, legal, risk and operational requirements. Therefore the Data Protection and Information Sharing Policy is part of the Information Governance suite and should be read in conjunction with our E-Safety Policy, Safeguarding Policy, Whistle Blowing Policy and legislation and guidance referred to above.

Introduction

Crockerne C of E Primary School collect and use personal information about staff, pupils, parents and other individuals who come into contact with the schools. This information is gathered in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The School, as Data Controllers, are registered with the Information Commissioner's Office (ICO) detailing the information held and its use. We issue a 'Data sheet to all parents, which summarises the information held on pupils this can be update by parents. Crockerne C of E Primary School will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data to ensure it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data

Any loss or misuse of personal data can have serious effects for both individuals with personal liability and / or institutions concerned, as it can bring the school into disrepute and may well result in disciplinary action and / or fines and/or criminal prosecution.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority. 2 The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles". (Please see Appendix 1 for Subject Access Request Procedures.)

Personal Information

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. The school has access to a wide range of personal information and data. The data may be held in different formats such as digital or paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include;

Personal information of a private or sensitive nature about members of the school community – including pupils, parents and carers, also members of staff and other professionals e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records;

- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references;
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, health forms and references;
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members and shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others

Information that is not already lawfully in the public domain.

Sensitive Personal

Data Sensitive personal data consists of information relating to the racial or ethnic origin of a data subject, their political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition, or criminal offences or record.

Where the school, as Data Controller intends to process sensitive personal data, there are further conditions. If none of the following conditions can be met, processing cannot legally continue;

- where the data subject has given his explicit consent;
- where the processing is required for the purposes of complying with employment law;
- where it is necessary to establish, exercise or defend legal rights.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

Crockerne C of E Primary School is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure our staff are aware of and understand the policy and procedures.
- Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Protective Marking

Although the school does not physically label documents using the Government Protective Marking Scheme, it is useful for staff, governors, and contractors working for it to have regard to the scheme to ensure that all parties comply with restrictions that apply to access to, handling and storage as well as the destruction of personal and sensitive data. The table below provides a useful guide:

	The information	The technology	Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extracurricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would

	be considered too sensitive to make available using other online means.		fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category
Learning and achievement	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. CHPs, Annual Reviews, Statement of Educational need, Child Data, Child Risk Assessments, Children's work, Home School Diaries, IEPs.	Currently paper based and posted. *Our ambition is to make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.*	Learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this learners record available in this way.
Safeguarding	Child Protection and Safeguarding information, Staff Support Records.		CONFIDENTIAL

Sensitivity of data	Impact Level (IL)	Likelihood of Risk				
		Very unlikely	Unlikely	Possible	Likely	Frequently

NOT PROTECTIVELY MARKED	0					
PROTECT	1 and 2	low	low	medium	medium	medium
RESTRICTED	3	low	medium	medium	medium	high
CONFIDENTIAL	4	medium	medium	medium	high	high
HIGHLY CONFIDENTIAL	5					

Emails containing data that falls into the PROTECT OR RESTRICT categories will be marked as such and will not be sent externally, except where the intended recipient is authorised to receive the email, the secure email system (using encryption) is used and the Headteacher has authorised the email.

All paper based PROTECT or RESTRICT (or higher) material must be held in lockable storage.

It is important to note that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach.

Identification of Data Assets & Risk Assessments

The SLT will identify and log data assets held by various users in the school – whether electronic, hard copy, or held in cloud storage. Information risk assessments will carried out to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences of a breach)

Risk Assessment is an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk Actions Form							
Information Asset Retention period	Information Asset Owner	Impact Level	Location of data asset	Likelihood of breach	Overall risk level (low, medium,	Action(s) to minimise risk	k Retention period

					high)		
Home address of child		RESTRICT		Possible	Medium	Raise awareness with staff re unintentional disclosure	
Learners data		PROTECT					
Staff Data		PROTECT					

The Business Manager (as Data Protection Officer) will maintain an inventory of, and will audit all school ICT equipment such as desktop and laptop computers and all portable devices e.g. cameras, iPads.

Members of staff who are leaving must return all personally-issued ICT equipment to the Business Manager. Staff who are leaving will be required to sign a declaration, countersigned by the Headteacher and Business Manager, confirming they have returned all school equipment and property, also that they will not attempt to access school information after their leaving date and that their personal ICT equipment will be appropriately configured to prevent unauthorised access to personal or sensitive information (see Appendix 2.

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system or to all records. All ICT users will be given secure accounts and must create strong passwords which must be implemented in accordance with the school's E-Safety Policy, regarding Password Security. Personal data may only be accessed on school devices which are securely password protected. *Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.* All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

The school promotes a clear desk approach to ensure information of a personal or sensitive nature is not available for unauthorised access. Personal data can only be stored on school servers or equipment (this includes computers and portable storage media where allowed). *No information of a sensitive nature can be kept on a*

member of staff's personal drive e.g. C:/ drive. Personal equipment (i.e. owned by the users) must not be used for the access or for the storage of personal data. It is the responsibility of the member of staff to ensure any personal equipment used to open school emails and attachments of a confidential nature by remote access, does not retain any information on the hard drive.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other multi-agency organisations. In these circumstances:

Users may not remove or copy RESTRICTED data from the school or authorised premises without permission from the Senior Management Team and unless the media is encrypted and password protected and is transported securely for storage in a secure location. CONFIDENTIAL information may only be removed with agreement from the Headteacher.

- Users must take particular care that computers or removable devices which contain personal data to ensure that they are not be accessed by other users (e.g. family members) in or out of school.
- When sensitive or personal data is required by an authorised use from outside the school's premises (for example, by a member of staff to work from their home), users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is school-issued, encrypted and is transported securely for storage in a secure location and returned to the secure area of the school onsite network.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Other secure options will be explored including use of secure remote access to the management information systems.

Remote/Cloud Storage and third party hosting

As a Data Controller, the schools are responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party. The schools are also aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

Destruction of Data

Crockerne C of E Primary School will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of data deemed protected or higher, in either paper or electronic form, will be conducted in a way that makes reconstruction highly unlikely. A normally deleted file can be recovered, even if the file is later overwritten by a new one. Electronic files will be securely overwritten (generally seven times as in 7 encrypted software), in accordance with government guidance and other media will be shredded, incinerated or otherwise disintegrated.

Information Risk Incidents

All data protection incidents, both breaches and near misses must be reported immediately to the Headteacher. An activity log recording the timeline of the incident management will be completed. The management response to any reported data security breach will involve the following four elements:

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

A plan of action to prevent recurrence and further awareness-raising will also be developed.

Disaster Recovery

The school has an Disaster Recovery Plan (see Crockerne C of E Primary School 's Financial Regulations and Procedures) that provides the framework for Crockerne C of E Primary School to develop a plan that considers the preparation for, response to and recovery from a disaster affecting all (or part) of the range of critical data held in the schools' management information systems.

Disclosure of educational records

Schools, as independent public bodies, are directly responsible under the Data Protection Act 1998 (DPA) for the collation, retention, storage and security of all information they produce and hold. This will include educational records, pupil reports and any other personal information of individuals - pupils, staff and parents. The Pupil Information Regulations 2005, require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided

and within 15 school days. Governing bodies can charge a fee for the copy but if they do, it must not be more than the cost of supply.

Information Sharing

Information Sharing is a key element of safeguarding children and young people. Crockerne C of E Primary School will explain to parents/carers what and how information will or could be shared, with whom and why and also seek their agreement when required. Personal information of a private or sensitive nature relating to children within a class is only for the use of the teacher, supply staff, and other staff or professionals, who need to know and who work with the child. It is the responsibility of the class teacher to ensure appropriate information is shared effectively, appropriately, legally and professionally. The personal information must only be shared with other professionals, relevant support staff or other teachers in this school for genuine purposes, for example, to seek advice on a particular case or ensure cover for work while on leave. It is the class teacher's responsibility to share confidential information appropriately, with their team both permanent and temporary. This is to ensure children's care, safety and well-being, so must be the overriding consideration in making any decisions. *Any decision to share, or not share, information must be recorded, detailing the reason for the decision, what information has been shared, with whom and for what purpose*. This record must be held with the child's record. If confidential information is shared, as outlined above, this must be in a professional 8 manner to ensure compliance with current Information Sharing Guidance and the Information Sharing Policy and protocols.

Whilst parents have a right to expect that personal information they share with Crockerne C of E Primary School will be regarded as confidential there are, however, certain circumstances when information can be shared without parents' consent, such as when there is evidence that the child is suffering, or is at risk of suffering, significant harm.

- there is reasonable cause to believe that a child may be suffering, or at risk of suffering significant harm.
- failing to do so would put a pupil at increased risk of significant harm,
- it would undermine the prevention, detection or prosecution of a serious crime.

When sharing information without consent, Crockerne C of E Primary School will always consider the safety and welfare of a pupil in making the decision. When there is a concern that a pupil may be suffering, or is at risk of suffering, significant harm, the student's safety and welfare will always be the overriding consideration. It is the responsibility of the designated Child Protection Officer to decide and provide authorisation to staff seeking to make a disclosure. If information is shared, this will be recorded in the student safeguarding file in the following way: What information

was provided and to whom, the reason for sharing information and the name of the Designated Child Protection Officer disclosing the information together with the member of the Leadership Team who authorised disclosure of information. All information shared will be in accordance with current Information Sharing Legislation and Guidance, also Data Protection Act principles of being up to date, necessary for the purpose for which it is being shared and shared only with people

Complaints

Complaints will be dealt with in accordance with Crockerne C of E Primary School 's Complaint's Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator). Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Apendix 1

Rights of access to information

There are three distinct rights of access to information held by schools;

1.Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them. This right is commonly referred to as subject access requests (SARs), is created by Section 7 of the Data Protection Act. It can be used by individuals who want to see a copy of the information the school holds about them. They can request to be;

- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

2.The right of those entitled to have access to curricular and educational records as defined within the Education Records Regulations 2005 and 2008. The Pupil Information Regulations require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided and within 15 school days. The procedures to follow are the same as for Subject Access Requests, however the time scales and fees differ. The Governing Body may charge a fee for the copy but if they do, it must not be more than the cost of supply – see section 4.

3. A Freedom of Information request can be initiated by any person. The information disclosed through an FOI request will usually become public information, available to anyone. The response cannot, therefore include personal or sensitive information, as these are exempt from FOI requests. This may be subject to a fee, to be determined, on a case by case basis by the Governing Body.

Handling a Subject Access Request, Pupil Information or Freedom of Information Request

1.Requests for information must be made in writing; which includes email, and be addressed to the Head teacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2.The identity of the requestor must be established before the disclosure of any personal or sensitive information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of at least two of the following, to establish identity and current address :

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into 10 account when making a decision. A child with competency to understand can refuse to consent to the request for their records to be disclosed. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Of the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Head teacher.
- Should the information requested be personal information that does not include any information contained within educational records the school can charge up to £10 to provide it.

5.The response time for Subject Access Requests, once officially received, is 40 calendar days (irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees, identification and clarification of information sought

6.The response time for Pupil Information requests, once officially received, is calendar 15 days (irrespective of school holiday periods). However the 15 days will not commence until after receipt of identification and clarification of information sought, if required.

7.The response time for Freedom of Information requests, once officially received, is calendar 15 days (irrespective of school holiday periods). However the 15 days will not commence until after receipt of fees and clarification of information sought

8.The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure by the Headteacher.

9.Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale for SARs.

10.Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

11.If there are concerns over the disclosure of information then additional advice should be sought.

12.Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

13.Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

14.Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Appendix 2

CROCKERNE C OF E PRIMARY SCHOOL FEDERATED SCHOOLS

Data Protection and Information Sharing Policy

School Staff - Leaver Data Protection Declaration

Please sign below to agree that:

- I have returned all school equipment and property
- I will not attempt to access school information after my leaving date
- I am not in possession of any personal or sensitive data relating to school
- My personal ICT equipment will be appropriately configured to prevent unauthorised access to any school personal or sensitive information

Name:

Signature:

Date:

Headteacher:
Signature:

Business Manager:
Signature: