Laurel Avenue
Community Primary School

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. (Refer to Becta: Good Practice in information handling in schools, 2009 – keeping data secure, safe and legal)

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

- *have permission to access that data, and/or*
- *need to have access to that data.*

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

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 protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'.

Privacy Notice

Privacy Notice can be found here:
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

Conditions for Processing

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. At least one of the following conditions must be met whenever you process personal data:

- *The individual who the personal data is about has consented to the processing.*
- *The processing is necessary:*
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.

- *The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).*
- *The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.*
- *The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.*
- *The processing is in accordance with the "legitimate interests" condition.*

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on 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 about members of the school community – including pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records*
- *Curricular/academic data e.g. class lists, pupil progress records, reports, references*
- *Professional records e.g. employment history, taxation and national insurance records, appraisal records and references*
- *Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members*

Responsibilities

The school's Senior Information Risk Officer (SIRO) is Ms G Davison, Headteacher. This person will keep up to date with current legislation and guidance and will:

- *determine and take responsibility for the school's information risk policy and risk assessment*
- *appoint the Information Asset Owners (IAOs)*

The school will identify Information Asset Owners (IAOs): Mrs J Lindsay, Admin Officer, Mrs J Ferguson, Admin Officer, Mrs H Walters, Deputy Headteacher for the various types of data being held (e.g. pupil information/staff information/assessment data etc.). The

IAOs will manage and address risks to the information and will understand:

- *what information is held, for how long and for what purpose*
- *how information has been amended or added to over time, and*
- *who has access to protected data and why*

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.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – The Privacy Notice

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents/carers when their child enrols in school. Parents/carers of young people who are new to the school will be provided with the privacy notice in the 'New Starter Pack'.

Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- *Induction training for new staff*
- *Staff Meetings/Professional Development Sessions*
- *Day to day support and guidance from Information Asset Owners*

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners 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) and*
- *Prioritising the risks.*

Risk assessments are an on-going process and should result in the completion of an Information Risk Actions Form:

Risk ID	***Information Asset affected***	***Information Asset Owner***	***Protective Marking (Impact Level)***	***Likelihood***	***Overall risk level (low, medium, high)***	***Action(s) to minimise risk***

Impact Levels and protective marking

Following incidents involving loss of data, the Government published HMG Security Policy Framework [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data.

The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	***Impact Level (IL)***
NOT PROTECTIVELY MARKED	*0*
PROTECT	*1 or 2*
RESTRICTED	*3*
CONFIDENTIAL	*4*
HIGHLY CONFIDENTIAL	*5*
TOP SECRET	*6*

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.
The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to and the handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware 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. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. 'Securely delete or shred this information when you have finished using it'.

Secure Storage of and access to data

The school has ensured 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.
All users will use strong passwords which must be changed regularly – once a term. See School's Password Security Policy. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected; the management machines in Headteacher's Office and Admin Officer's office. 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.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data. Every member of staff is issued with an encrypted, password protected data stick which must be used for the storing of any personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media

- ♦ *the data must be encrypted and password protected,*
- ♦ *the device must be password protected*
- ♦ *and the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.*

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. ICTSS organises the backing up of the admin and curriculum servers with reports delivered to the school's secure e mail address daily for the admin server. The Admin Officer checks daily that the curriculum server has been backed up successfully. ICTSS are responsible for accessing and restoring data held in school.

All paper based Protected and Restricted (or higher) material is held in lockable storage – locked filing cabinets in office, staffroom and Foundation Stage Classroom.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data. Parents/Carers may request to see a copy of the information held about them and their child/ren. Requests are made to Mrs Lindsay, Admin Officer. This right to request is clearly *indicated in the Privacy Notice given to all Parents/Carers when their child enrols in school and is included in the 'New starter Pack' as well as the list of other agencies with whom this data may be shared.*

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 agencies. In these circumstances:

- *Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location*
- *Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school*

  When restricted or protected personal data is required by an authorised user from outside the organisation's
  premises (for example, by a member of staff to work from their home),they should have secure remote access to
  the management information system or learning platform, Durham Learning Gateway
- *If secure remote access is not possible, 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 encrypted and is transported securely for storage in a secure location*
- *Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)*

(Detailed guidance on data encryption is found in the Becta document 'Good practice in information handling in schools – Data Encryption - a guide for staff and contractors tasked with implementing a system of secure data encryption and deletion'):
http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.
The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging/Reporting/Incident Handling

Schools will find detailed guidance on audit logging in the Becta document "Good practice in information handling in schools - audit logging and incident handling - a guide for staff and contractors tasked with implementing data security": http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

It is good practice, as recommended in the 'Data Handling Procedures in Government' document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals; Ms G Davison, Headteacher, Mrs H Walters, Deputy Headteacher and Mrs J Lindsay, Admin Officer, Mrs J Ferguson, Admin Officer.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	***The technology***	***Notes on Protect Markings (Impact Level)***
School life and events	*School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events*	*Common practice is to use publically 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.*
Learning and achievement	*Individual 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.*	*Typically schools will 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*	*Most of this information will fall into the PROTECT (Impact Level 2) category.* *There may be pupils 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*

		belonging to the parent.	*school may decide not to make this pupil record available in this way.*
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 be considered too sensitive to make available using other online means.*	*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 fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.*

Appendices: Additional issues/documents related to Personal Data Handling in Schools:

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- *For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.*
- *They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.*
- *They must provide alternative means for accessing services where a parent or pupil has refused consent.*

Freedom of Information Act

Laurel Avenue Community Primary School has a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- *Delegate to the Headteacher day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.*
- *Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.*
- *Consider arrangements for overseeing access to information and delegation to the appropriate governing body.*
- *Proactively publish information with details of how it can be accessed through a Publication Scheme and review this annually.*
- *Ensure that a well-managed records management and information system exists in order to comply with requests.*

Model Publication Scheme

This publication scheme has been prepared and approved by the Information Commissioner. It has been adopted by Laurel Avenue Community Primary School. The school's publication scheme should be reviewed annually.

Privacy Notice
for
Laurel Avenue Community Primary School

Privacy Notice - Data Protection Act 1998

Laurel Avenue Community Primary School *is a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:*

- ♦ *Support its pupils' teaching and learning;*
- ♦ *Monitor and report on their progress;*
- ♦ *Provide appropriate pastoral care, and*
- ♦ *Assess how well the school as a whole is doing.*

This information includes contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE) and to agencies that are prescribed by law, such as the Qualifications and Curriculum Authority (QCA), Ofsted, the Learning Skills Council (LSC), the Department of Health (DH) and Primary Care Trusts (PCT). All these are data controllers in respect of the data they receive and are subject to the same legal constraints in how they deal with the data.

If you want to see a copy of the information about you that we hold and/or share, please contact Mrs Lindsay, Admin Officer.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

www.durham.gov.uk/dataprotection   and

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

Signed: G Davison

Headteacher
Date: October 2016

Signed: C Linfoot

Chair of Community and SMSC Committee
Date: October 2016

Review: October 2019