ETTINGTON CE PRIMARY SCHOOL

DATA PROTECTION POLICY

DATA PROTECTION POLICY

1.DATA AND THE DATA PROTECTION ACT 1998

1.1 The Data Protection Act 1998 requires all organisations including schools that handle personal information to comply with a number of important principles regarding privacy and disclosure. The Act states that anyone who processes personal information must comply with eight principles making sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

1.2 Personal information is a combination of any data that identifies an individual and gives specific information about them, their families or circumstances. It can be held electronically or on paper.

1.3 Ettington Primary School will comply with the terms of the 1998 Data Protection Act, and any subsequent relevant legislation to ensure personal data is treated in a manner that is fair and lawful. Ensuring fairness in everything the Federation does with people's personal details is central to complying with the duties under the Data Protection Act. In practice, it means that each school must:

- have legitimate reasons for collecting and using personal data
- not use data in ways that have unjustified adverse effects on the individuals concerned
- be open and honest about how the data will be used and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect
- not do anything unlawful with the data

1.4 Fairness generally requires transparency. There will be clarity and openness with individuals about how their information will be used.

1.5 To comply with the Act, the school is registered as a data controller and employees, parents and volunteers will be issued with a privacy notice annually: parents will have this attached to the data collection sheets.

1.6 Information and guidance can be found on the Information Commissioner's website
http://www.ico.gov.uk

1.7 This policy should be read in conjunction with the Warwickshire Information Sharing Agreement (Appendix 1).

2. DATA GATHERING

2.1 All personal data relating to staff, pupils or other people with whom Ettington Primary School has contact, whether held on computer or in paper files, is covered by the Act.

2.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

3. DATA STORAGE

3.1 The Head Teacher shall decide which employees within each school should have access to the various levels of data held and shall appoint individual staff to oversee the management of areas of data who understand what information is to be held and for what purpose, how it will be stored, who has access to it and why and how it will be retained and disposed of.

3.2 In addition to the Head Teacher, the relevant areas and appointed persons are:

Designated Safeguarding Leads:
Michelle Crowe, Abby Solomon
SEND:
Isobel Stanley, Elaine Marney
Assessment:
Michelle Crowe
School Management Systems:
Lorraine Holmes
HR:
Lorraine Holmes
Finance
Lorraine Holmes

3.3 Personal data will be stored in a secure and safe manner. Electronically, data will be protected by standard password and firewall systems operated by each school. Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.

3.4 Staff access will be restricted according to their level of responsibility and the scope of their job description. Information is stored on SIMS.

3.5 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.

3.6 Particular attention will be paid to the need for security of sensitive personal data.

4. DATA CHECKING

4.1 Each school will issue annual requests to staff and parents for up to date information and shall issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

4.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

5. DATA DISCLOSURES

5.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data or organisations that have a legal right to receive the data without consent being given.

5.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

5.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

5.4 Requests from parents or children for printed lists of the names of children in particular classes should be politely refused as permission would be needed from all the data subjects contained in the list.

5.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
5.6 Routine consent issues will be incorporated into each school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

5.7 Personal data will only be disclosed to Police Officers if they need some information to prevent or detect crime or catch or prosecute a suspect. However there are limits on the information that can be released. If the Head Teacher is satisfied that the information is going to be used for this purpose and that if the information was not released, it would be likely to prejudice (that is, significantly harm) any attempt by the police to prevent a crime or catch a suspect, then he can authorise disclosure.

5.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

5.9 Particular attention shall be paid when faxing documents. The recipient must be telephoned and the fax number confirmed. The location of the fax machine should be established. The facsimile should then be sent and the recipient telephoned again to check receipt of the document.

6. SUBJECT ACCESS REQUESTS

6.1 If Ettington Primary School receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond in accordance with the requirements of the Act.

6.2 Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond.

6.3 Should parents request data from their child's educational record, the Governors shall refer to Guide to the Law for Governors:

Material in the pupil's educational record exempt from disclosure to parents:
Para 44. When schools comply with a parent or carer's request to see or have a copy of a pupil's educational record under the Education (Pupil Information) England) Regulations 2005, there is some information that must not be disclosed. This is any information that may not be given under the Data Protection Act 1998 or to which he or she would have no right of access under that Act or by virtue of any order made under Section 30(2) or Section 38(1) of the Act.

The following information must not be disclosed:

- *Information, the disclosure of which would be likely to cause serious harm to the physical or mental health or condition of the child or someone else;*
- *Information as to whether the child is or has been subject to or may be at risk of child abuse, where the disclosure of that information would not be in the best interests of the child;*
- *References supplied to potential employers of the child, any national body concerned with student admissions, another school, an institution of further or higher education, or any other place of education and training;*
- *Information supplied by the school in a report to any juvenile court, where the rules of that court provide that the information or part of it may be withheld from the child;*
- *Information recorded by the pupil during an examination;*

• *Information concerning the child that also relates to another person who can be identified from that information, or which identifies another person as the source of that information, unless the person has consented to the disclosure, or it is reasonable in all the circumstances to disclose the information without his or her consent, or the person is an employee of the LA or of the school. (This exemption does not apply where it is possible to edit the information requested so as to omit the name or any other identifying particulars of that other person.)*

7. LOSS OF DATA

7.1 If, despite security measures taken to protect personal data held, a breach of security occurs, the breach will be dealt with effectively. The breach may arise from a theft, a deliberate attack on the school systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. However the breach occurs, it will be managed appropriately. A strategy shall be applied by the Head Teacher including:

- a recovery plan, including damage limitation
- an assessment of the risks associated with the breach
- informing the appropriate people and organisations that the breach has occurred
- a review and update of the school information security systems.

8. PENALTIES FOR BREACH

8.1 Notwithstanding the above, the handling of data is everyone's responsibility. Failure to comply with appropriate controls to secure data could amount to gross misconduct or may lead to legal action.

8.2 Staff are referred to Appendix 2 for a list of recommendations on how to reduce the risk of information going missing or being obtained illegally.

APPENDIX 1

Warwickshire Information Sharing Agreement April 2011
INTRODUCTION AND PRINCIPLES

This document sets out an information sharing agreement between the Local Authority (LA) and partner educational institutions including maintained schools, academies and colleges in Warwickshire.

The Local Authority and educational institutions in Warwickshire share information to enable the LA to fulfil its statutory obligations, to discharge its democratic mandate for oversight of children's welfare and progress, and to provide comparative statistical data to support professional development and improvement. All concerned agree that no elected member or officer of the LA, no governor, headteacher, principal or

member of staff in a partner institution, and no other colleague with access to the data will make any public value judgement or compare performances of named institutions on the basis of data or other information shared under this agreement.

DATA MANAGEMENT

All data exchange and storage will adhere to the Data Security Standards (ISO 17799). This provides both sides of the partnership with the assurance and satisfaction of knowing that they are protecting their information using controls in common use by well-managed organisations.

Further information is available on the website http://www.standardsuk.com/.
For the LA, data is normally managed by its commissioning support service (CSS), which can be contacted by emailing css@warwickshire.gov.uk.

Under the Data Protection Act 1998, all public organisations that hold individual data must be registered with the information commissioner. This includes schools, colleges and academies, and information that is held electronically or on paper. These organisations are deemed "data controllers", and are responsible for the secure storage and distribution of that data. It is the responsibility of the data controller to ensure that the organisation is registered with the Information Commissioner and that all individual person data usage and storage adheres to the principles of the Act. Further information can be found on the

Information Commissioners website http://www.ico.gov.uk/ or by contacting their helpdesk on (01625) 545745

When pupils transfer between maintained schools, the school has a statutory duty to transfer pupil data to the new school electronically. This should be done by creating a common transfer file and sending it to the DfE's school 2 school transfer site: https://securedatatransfer.teachernet.gov.uk/sdtlive/asp/Login.asp.
For further information on how to do this, please contact the LA's ICT Development Service Helpdesk on (01926) 414100.
All data sets must have an owner, and ownership of data sets must be clear, particularly if they are shared or if ownership is transferred. Data owners are responsible for the upkeep and accuracy of their data sets, for dealing with any uncertainties and irregularities, and for responding to any requests under the Freedom of Information Act.

DATA AND INFORMATION COLLECTED

At the time of writing, the LA expects to receive the following individual pupil level data sets:

- Spring, summer and autumn school census collections. The LA collects this data directly from all maintained schools, while academies send their data to the Department for Education (DfE), which will forward a copy to the LA

provided it has received permission from the individual academy. The LA will endeavour not to make any additional data collections during the year that duplicate pupil data collected via the school census.

• Early Years Foundation Stage Profile and Key Stage 1 assessments. Maintained infant and primary schools return their assessments to the LA annually in June.

• Key Stage 2 and 3 results. These results are provided by the DfE on its Key to Success website. The first release of provisional data is normally in July with further releases from August onwards.

• Key Stage 4 and Post 16 examination results. These are obtained by the DfE from examination boards and awarding bodies. The LA subscribes to the National Consortium for Examination Results (NCER), which provides analyses of results for all institutions including academies and colleges that have signed permission letters.

This data includes all eligible pupils in maintained schools. It also contains pupil data from academies and colleges that have signed permission letters. The first release of data is normally in October with further releases from November onwards. The LA makes appropriate analyses available through the secure We-Learn website.

• Fischer Family Trust (FFT) data. The LA pays a subscription to the Fischer Family Trust in order to receive FFT analyses of actual results, and FFT estimates for future results of individual pupils and students. The LA receives data for all individual pupils in maintained schools, and can also receive data for academies and colleges that have signed specific permission letters. At the time of writing, college data does not include data for individual students. FFT data is made available through the secure FFT Live website, and updates are issued throughout the year.
• Year 11 destinations data. This lists all Year 11 pupils from all establishments across Warwickshire (including maintained schools, independent schools and academies) highlighting the “destination” of each young person as at November after the July they have left school. In the past, this data has been received securely from Connexions annually in January.

•Summer holiday collections of headline results. Schools and colleges are asked to make a provisional return of headline data on A Level and GCSE results days in August. This does not contain individual pupil data. It is used to inform the LA and no results for individual institutions are made public.

• RAISE online full reports and interactive website. The LA uses RAISE online information, but has no responsibility for the data itself, which is made available by Ofsted on the RAISE online website www.raiseonline.org.uk. It is able to see the results at individual pupil level, but only in anonymous form.

Any questions about passwords or the data on this site should be addressed to Ofsted.

• Post-16 data in the learner achievement tracker, the data dashboard and the Ofsted post-16 PANDAs. Individual student level data for these data releases is collected directly from colleges by the Young Persons Learning Agency (YPLA).

DATA ANALYSIS AND INTERPRETATION

It is a cliché, but before data can be used in decision-making it needs to be converted into information. Hence, the individual and institution data collected above is aggregated to LA level and analysed, for example, by district, area, type of establishment, pupil group, and in relation to LA statistical neighbour and national performance. The LA uses performance data to inform its short-term actions, to provide a detailed appreciation of local circumstances in its needs assessment data, and to inform longer-term action plans including its Children and Young Peoples Plan.

MAKING DATA AVAILABLE TO INSTITUTIONS

Data on individual pupils is not shared with other institutions, and is only made available to their home institutions through the secure FFT and We-Learn websites. Analyses of aggregated data are made available to elected members, officers and partners of the LA, and to the institutions that have contributed data. Analyses produced by the LA are normally published by the LA's commissioning support service on the school information system (SIS) on the Warwickshire Learning Platform (WeLearn365).

Colleagues in maintained schools have WeLearn365 usernames and passwords, and accounts can be created for colleagues in academies and colleges if a request is made to the ICTDS Servicedesk.

Only colleagues authorised by their institutions will be able to access the school information system to see and download any data. These authorised users will see comparative data for other institutions at a summary level, but will only see data on individual learners for their own institution. Once downloaded, it is the institution's responsibility to share data only in accordance with the data sharing principles in this document. Senior leaders will generally limit access to those colleagues engaged in institution management, development and planning, taking appropriate care for the security of the institution's data on individual learners.

Some aggregated performance data may be made available by Warwickshire LA to partners of the LA, officers of other LAs and officers of other public bodies such as district councils. This will only be for the purpose of improving educational or other provision for children and young people. It will be on the specific understanding that recipients abide by this agreement and that they agree reciprocal arrangements so that Warwickshire institutions may benefit from access to data which they hold, and assist in strategies for improving provision.

Some individual level data is shared securely within the LA to support system and institution improvement and effectiveness. For example pupil characteristics data may be used to help set corporate priorities, to undertake geographical analysis including deprivation research, to populate the pupil forecasting system and to aid school place planning and commissioning. No data made available more widely will identify or make it possible to identify any individual pupil based in a Warwickshire institution.

REFERENCES

Information Commissioners website: http://www.ico.gov.uk/
The Data Protection Act: http://www.legislation.gov.uk/ukpga/1998/29/contents
Government Information Management Strategy: http://www.teachernet.gov.uk/Management/tools/ict/IMS/
Electronic Government Interoperability Framework (e-GIF): http://www.govtalk.gov.uk/interoperability/egif.asp

APPENDIX 2

WORKING ONLINE

Do

• make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and antispyware).

Get advice from your IT team if you need help.

• only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.

• turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)

• make sure that you only install software that your IT team has checked and approved

• be wary of links to websites in emails, especially if the email is unsolicited

• only download files or programs from sources you trust. If in doubt, talk to your IT team.

• check that your organisation has an acceptable-use policy (AUP) for the internet and ensure that you follow it.

EMAIL AND MESSAGING

Do

• report any spam or phishing emails to your IT team that are not blocked or filtered

• report phishing emails to the organisation they are supposedly from

• use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

Don't

• click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.

• turn off any email security measures that your IT team has put in place or recommended

• email sensitive information unless you know it is encrypted . Talk to your IT team for advice.

• try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)

• reply to chain emails.

PASSWORDS

Do

• use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)

• make your password easy to remember, but hard to guess

• choose a password that is quick to type

• use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

Don't

• share your passwords with anyone else

• write your passwords down

- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

LAPTOPS AND iPADS

Do

- shut down your device using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your device securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- Use the passcode feature on your iPad to stop unauthorised access
- make sure your laptop is protected with encryption software.

Don't

- store remote access tokens with your laptop
- leave your device unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your device in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your device
- use hibernate or standby.

SENDING AND SHARING

Do

• be aware of who you are allowed to share information with. Check with the Head

Teacher if you are not sure.

• ask third parties how they will protect sensitive information once it has been passed to them

• encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

Don't

• send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available

• send sensitive information by email unless it is encrypted (Welearn365 is encrypted)

• place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.

• assume that third-party organisations know how your information should be protected.

WORKING ON SITE

Do

• lock sensitive information away when left unattended

• use a lock for your laptop to help prevent opportunistic theft.

Don't

• let strangers or unauthorised people into staff areas

• position screens where they can be read from outside the room.

WORKING OFF SITE

Do

• only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.

• wherever possible access data remotely instead of taking it off-site

• be aware of your location and take appropriate action to reduce the risk of theft

• make sure you sign out completely from any services you have used

• try to reduce the risk of people looking at what you are working with

• leave your device behind if you travel abroad (some countries restrict or prohibit encryption technologies).

SIGNED : …….

DATE : ……..