Merrydale Infant School Data Protection Policy

Chair's signature Mrs E Surtees

Head's signature…Mark Tipple-Johnson

Date……31st October 2023

Review date……October 2024

The Data Protection Act 1998 came into force on 1st March 2000. The Act Statement/ places obligations on the way 'data controllers' such as schools 'process' personal data. Personal data is any information that covers records relating to pupils and members of the school staff.

Schools must notify the Information Commissioner what personal data they hold and state the purposes for which it is required to be held. Failure to notify is a criminal offence. If a school's notification entry becomes inaccurate or incomplete, the school must inform the Information Commissioner of any relevant changes within 28 days. Failure to do so is a criminal office.

Processing data held under the Act other than in full accordance with the law is also a criminal offence – one for which both the school as a body and the individual responsible can be prosecuted. Personal data now covers information held in 'structured' paper filing systems or other accessible paper records as well as computerised records.

The over-arching principles of the 1998 Act include:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    a) At least one of the conditions in Schedule 2 is met, and
    b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one of more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.Staff records will be held securely in the head teacher's office.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data..
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 protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This means that when personal data becomes out of date, or no longer relevant to the purpose for which is was originally collected, it must be destroyed.

Schools must give the Information commissioner a general description of the measures taken to prevent unauthorised access to, or disclosure of, personal data. Basic security steps should be taken to ensure that the general public, unescorted visitors and unauthorised personnel are restricted from areas where personal data is used.

Any member of the school staff who deals with personal data as part of their job should be aware of the requirements of the Act and be familiar with how to conform to these in their daily work.

The Data Protection Act gives any person whose personal data is held by the school, regardless of whether they are an adult or not, the right to access that data. Requests to see or receive copies of records should be made in writing to the Headteacher. Parents can

also exercise this right of access to the official educational records of their children. Again, formal requests should be made in writing to the Headteacher.

Publication of personal information or images of individuals on any Web Site schools develop should only be done if the written consent of the individuals concerned has been given.

E-mail should never be treated as a secure method of communication when dealing with personal data as defined by the Data Protection Act. Do not include personal or confidential information in the text of e-mails (or attached as a data file) to be sent outside the school unless appropriate encryption is applied to protect it.

A new requirement of the 1998 Act is the inclusion of a definition of sensitive personal data, which consists of information as to:

- The racial or ethnic origin of the Data Subject;
- Their political opinions;
- Their religious beliefs or other beliefs of a similar nature;
- Whether they are a member of a trade union;
- Their physical or mental health or condition;
- Their sexual orientation;
- The commission or alleged commission by them of any offence, or,
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings;
- Explicit consent must be obtained to process this type of data.

Organisation: 1. On occasion it is necessary for the school to work with outside agencies for the benefit of a student. This will necessitate the need for sharing information. The school will ensure that only relevant information is disseminated to other agencies and will also ensure that such processing is lawful. If necessary, the school will check to ensure the person receiving the information is from a bona-fide organisation.

2. Information from Annual/Transitional Reviews will only be given to the relevant organisations and parents.
3. The performance and destination of individual students will not be identified in any school publication that is distributed beyond the school staff.
4. The school will not divulge the names, addresses or other confidential information about any students or staff. Staff should be mindful that this information should not be displayed openly.
5. Parental permission will be sought before students' photographs or articles concern them appear in any media publications.
6. Staff records will be held securely in the head teacher's office. Staff may only have sight of their own records.

7. Pupil records will be held securely in the SEN office. These may not be taken off the school site. If staff wish to borrow a particular student file it must be signed out and only used within the school area.
8. Records of classroom observations and performance data will be held by the Senior Leadership Team and only shared with the individual concerned.
9. Information on candidates applying for jobs at the school will be retained for 12 months and then destroyed.
10. All confidential information relating to staff or students will be destroyed by shredding.
11. Governors will not have an automatic right to information on any member of staff or student. In the case of exclusions or complaints, members of the governors' panel will only be furnished with the necessary information for them to make an informed judgement on the specific incident.

Monitoring & Evaluation: This policy should be reviewed annually with a report to the governing body.

Responsibilities: Operational responsibility for ensuring that a school complies with the Data Protection Act lies with the Headteacher. The governing body, however, needs to have an overall appreciation of the requirements of the Act so that it is in a position to ensure that the school is conforming to the law on an ongoing basis.

Relation to Other Policies: This policy relates to all other policies where recording of pupil levels and achievements are noted. It is also relevant to staff professional development.

Introduction Any incident involving the loss, suspected loss, or exposure of data in electronic format, must be reported in order that appropriate investigation is made, risk countermeasures implemented and lessons learnt to prevent reoccurrence. Therefore any loss of ICT equipment that stores work related files must be reported (such as Laptops or Memory Sticks). This will then allow the school to check governance arrangements for data, and to decide whether the breach needs to be reported to the Information Commissioner's Office (ICO), who is empowered to require action on the part of the school.

1. **Review and Maintenance** This policy will be subject to annual review by the Governors Health and Safety committee. It will be re- submitted, along with the staff AUP, at the beginning of every academic year.

2. **Reporting Requirement** Any actual or suspected loss, either in school or externally, must be reported and investigated. The person discovering or suspecting the loss must in the first instance report it to the headteacher who will then interview the necessary people and produce an initial Damage Assessment. In consultation with the chair of governors, it will then be decided within 24hrs as to whether the potential breach should be reported to the ICO.

If the breach is considered to be negligent, Personnel will be informed.

All reports must be made using the Data breach form, attached to this document.
Losses of ICT equipment and media must be reported in this manner, even if you believe that no data loss is involved.

Data Security Breach Report

Form – Please complete and hand it to the head teacher

NAME:	DATE:
	Job Title:
Nature of the Incident: Include: Date, time and location of incident Description of what happened Theft, accidental loss, inappropriate disclosure.	
Brief description of Item/data lost: eg: Personal, Financial, Register etc. Also indicate volume of data eg number of records, files, discs etc.	
Number of individuals potentially affected: This could be either staff, pupils or both	
Information format: Electronic media, devices (laptops, phone, tablet, USB Memory Stick, cd/dvd etc, note if the device is encrypted.	
Initial Actions taken: Have you asked anybody, or do you have any suspects or situations?	
Damage Assessment (to be completed by the headteacher)	

Laptops and Mobile Devices e.g. Ipads Policy

Introduction

Although staff laptops are a huge asset, they represent a potential risk, to both data, and the school network. As such they and any data stored on them must be managed securely.

The aim of the policy is to support staff when they use Merrydale laptops in school or at home, by ensuring they are aware of the information security issues with which they must comply.

This policy should be read in conjunction with:

- Acceptable Use Policy (AUP).
- Data breach policy.
- Data breach form.
- Data guide for portable ICT equipment.
- Laptops Policy.
- Laptop Health & Safety information.
- Merrydale Infants Data Protection Policy

Compliance with the requirements of those policies is essential.

1. **Applicability** This policy covers the use within the school of all school laptops and other portable computer devices that you may have been given permission to use for work. These could include items such as; Notebooks, Ipods, I Pads , tablets, and smart mobile phones (those with internet/email).

2. **Review and Maintenance** This Policy will be subject to annual review by the governors. It will be re-submitted for signature by all staff in conjunction with the Acceptable User Policy at the beginning of every academic year.

3. **Risks**

Given their size and portability, laptops (and the data on them) are easily lost or stolen.

A. Unless devices are regularly monitored and receive anti-malware updates, they represent a substantial risk to the school network when reconnected.

B. There is also a risk of interception of data during the synchronisation process, particularly if either infrared or wireless links are used. Similarly if used in a public or other non-work environment there is a risk of oversight of data on screen.

C. personal devices must not be connected to the data network as they represent an unknown level of risk over which the school has no direct control. Personal equipment must never be used for connection to the data network nor for the storage of School data, be that personally identifiable data or not. If, for operational purposes, connection is unavoidable, permission must be sort from the head teacher first.

4. **Physical Security**

A. All Merrydale Infants mobile devices must be security marked and registered to the school.

B. Mobile devices should be out of sight during transportation. They should also be transported in a case designed for that purpose, if issued.

C. When not in use, mobile devices must be securely stored out of sight (whether at home or at school).

D. Where available, all devices should be accessed through a PIN/Password system.

5. **Technical Security**

A. The security software should never be turned off by a user.

B. The only method of external connection to the school network is through the laptops issued to staff, unless express permission has been granted by the headteacher.

C. All mobile devices must have up to date malware protection. Laptops come with security installed.

D. In the unlikely event that your Laptops contracts a virus:

- Turn the device off.

- Place a label over the switch stating that the machine has a virus infection and should not be used.
- Isolate any removable media e.g. FDs, CDs, USB memory sticks that have been used on that machine.
- Inform our Technician immediately or the Computing coordinator.

E. All mobile devices require operating system and other application software updates and vulnerability patches to be applied. This will happen whenever you connect to the network (through wireless or cable). It is your responsibility to ensure this is done conscientiously.

F. The Laptops are set up for work purposes. Software is allowed to be installed without the permission of the head teacher first (whether from a portable source, or from the internet), but there should be a good educational/work reason for doing so. If this system is abused, the equipment will be withdrawn.

6. **Data Security**

A. Your Laptops are fitted with appropriate full hard drive encryption.

B. Users must never store their passwords on the Laptop and/or any memory card (this includes keeping a copy in the vicinity).

C. Users must not store software serial numbers or passwords on their Laptop and/or memory card.

D. Users must regularly back up data to their network drive.

7. **Losses and Confidentiality/Security Breaches** Incidents that constitute a Loss of Hardware or Data are to be reported to the headteacher . Other security related incidents such as :
- Virus attacks
- Unauthorised access.
- Misuse of System/Privileges.

should also be reported in the same way.

8. **Negligence** Please be aware that if, through negligence, the equipment you are issued with is lost, damaged, or stolen, Personnel may be informed which could result in a disciplinary investigation.

9. **Secure Disposal and Re-use** Merrydale Infants follows a policy of safe, environmental recycling. We follow the Waste electrical and electronic equipment directive (WEEE). All equipment is therefore disposed of in a safe manner, through reputable, registered companies.

Display Screen Equipment - Laptops H&S Employee Information Sheet Issue 1 (April, 2005)

Introduction

This document contains general information and guidance on potential health and safety issues arising from the use of laptops. A separate information sheet is available on
'desktop' Display Screen Equipment.

Workstation Set-Up and Activities

Posture

- Avoid positioning the laptop right on the edge of the desk, as this causes you to look down excessively and therefore put your head and neck in a poor position.
- Avoid slouching and sitting forward in a slouched position.
- Try not to lean or bend to one side as this can put strain on your lower back.
- If you have screen glare move away to a spot where there is little reflection, adjust your screen brightness. Try not to sit with your back to, or face a window.
- Check your posture at regular intervals – you may start in a good position but change once you become engrossed in your work.

Wrists and Mouse Work

- Avoid sitting too high or too low to minimise the risk of strain injuries, particularly bending your wrists upwards and downwards when keying. Ensure that your forearms are roughly horizontal.
- Use a height adjustable chair when available to achieve this.
- Always try to use a mouse or glide pad so that your hand is flat and fingers are relaxed.

Home and Car

- Avoid using your laptop on a sofa, easy chair or coffee table.
- Avoid using your laptop whilst sitting in a car. If necessary, sit in the front passenger seat and push the seat back far enough to get as much space as possible.
- Use a flat stable item such as the computer case to raise the laptop and improve your posture as much as possible.

Work Breaks

- You should rotate your work activities wherever possible, to avoid long and uninterrupted periods of constant DSE use.
- If you do have long uninterrupted periods of DSE use, ensure you take a regular breaks to do other work tasks not involving screen/keyboard work. (As a general rule, 5-10 minutes for each 50-60 minutes continuous screen and/or keyboard work.)

Lifting and Handling

- Try to avoid taking hard copies of documents that may already be stored on your laptop.
- Always try to use a carry case with a padded shoulder strap or use luggage that has wheels where appropriate.
- Avoid carrying other loads in addition to the laptop.

Electrical safety

- Check the laptop lead and plug visually before you connect it and don't use the lead/plug if they look worn or damaged.

Security

- Reasonable precautions must always be taken (e.g. not leaving laptops on display in unattended vehicles).
- Keep equipment out of sight when driving by storing it in the boot.

Docking stations

- Docking stations are a separate monitor and keyboard, which a laptop can be connected to.
- If you regularly use laptops for long and uninterrupted periods, a docking station at your main desk/base should be provided if a 'desktop' PC is not available.

Health Issues
Some people may experience temporary discomfort in their upper body, especially after long periods of uninterrupted display screen work. In a very few cases aches and pains may become more persistent. Good workstation layout and good working practices can prevent most problems of this kind.

Entitlement to Eye Tests
The Display Screen Equipment Regulations define the term DSE 'User' as an employee who habitually uses display screen equipment as a significant part of their work. If you are identified as a DSE 'User' then you are entitled to an eye test and, where prescribed, spectacles. Your Manager or can provide you with further details about this.

Reporting problems
If you experience any ill-health symptoms (aches, pains) that you think may be related to DSE use, please report them to the headteacher. Persistent symptoms should be recorded on an SO2 incident report form.

Common Problems Common Solutions:
Tingling, pain or numbness in fingers of thumbs? Are you working with your wrists bent? You might be sitting too high or too low.
Stiff or aching neck Check the height of your monitor. Your eyes should be roughly level with the top of the casing.
Pain, swelling, tenderness and redness of hand, wrist and or forearm
Are you carrying out repetitive tasks for long, uninterrupted periods? Take short and frequent breaks form repetitive tasks to do different work.

Are pregnant women at risk from display screens?
Although this is a often expressed concern, there is no risk of miscarriage or foetal damage as the radiation levels from display screens are so small as to be totally harmless.
However, since anxiety can represent a danger in itself, pregnant women should discuss their concerns with their manager in the first instance.

Data guide for Portable ICT equipment e.g. Laptops and Ipads

Introduction *This guide is designed to act as a reminder about Data Protection at the Merrydale Infants . It offers a common sense approach to helping you enforce both the Staff Acceptable User Policy (AUP) and the Data protection Policy .*

1. **Data** Guidelines from the Information Commissioners Office (ICO) are very clear:

A. The data you transport on either your laptop or memory stick must be relevant to the work you are doing at the time.

B. Remember, always think 'do I have a good reason for having this data off site?'

2. **Passwords**

A. Passwords should be between 8 and 16 characters in length, a mix of letters and numbers. They should also be a mix of upper and lower case.

B. Users must never store their passwords on the Laptop and/or any memory card (this includes keeping a hard copy in the vicinity).

C. Users must not store software serial numbers or passwords on their Laptop and/or memory card.

3. **Software**

A. Unless devices regularly receive software patches and anti-malware and security updates, they represent a substantial risk to the school network when reconnected. This will happen whenever you connect to the network (through wireless or cable). It is your responsibility to ensure this is done conscientiously.

B. Your Laptops come with security installed. If you wish a copy for your home equipment, we can advise.

C. The laptop security software should never be turned off by a user.

D. The Laptops are set up for work purposes. Software is allowed to be installed without the permission of the Technicians first (whether from a portable source, or from the internet), provided it is for educational/work purposes, and can be justified if asked. If this system is abused, the equipment may be taken away from you.

E. Nobody else, either at work, or at home, has permission to use your allocated laptop. You will have the laptop taken from you if you don't abide by this rule.

F. In the unlikely event that your Laptops contracts a virus:

- Turn the device off.
- Place a label over the switch stating that the machine has a virus infection and should not be used.
- Isolate any removable media e.g. FDs, CDs, USB memory sticks that have been used on that machine.
- Inform the Technicians, either by coming into the ICT office, or by emailing cmits-csmleicester@capita.co.uk

4. **Network**

A. If you are accessing the school network wirelessly (either in school, or externally), someone may be trying to intercept the data, or may be looking over at the screen. Be vigilant.

B. Laptops should be accessed at all times through a PIN/Password system.

C. Users must regularly back up data to their network area.

5. **Transport & Storage**

A. When not in use, laptops must be securely stored out of sight (whether at home or at school).

B. Laptops should be out of sight during transportation. In order to minimise physical damage, they should also be transported in a case designed for that purpose.

6. **Losses and Confidentiality/Security Breaches** Incidents that constitute a Loss of Hardware or Data are to be reported to the headteacher. Other security related incidents such as Virus attacks, Unauthorised access and Misuse of System/Privileges should also be reported in the same way.

7.**Negligence** Remember, if you don't apply the school policies, as well as a little common sense, you may be negligent and therefore subject to legal action. Please be sensible and practice what the school policies ask you to.

User Signature I acknowledge that I have read and can access copies of:

- The Acceptable Use Policy (AUP).
- The Data protection Policy including laptop policy

I understand that these policies need to be implemented. I am aware that if I breach these policies, I may be liable to school discipline procedures and possible legal action

Signed……Date……

Full Name……..(printed)

Job Title……..

Information for staff regarding the School Data Protection Policy

The following is a summary of points staff ought to be aware of –

- The policy covers the use within the school of all school laptops and other portable computer devices that you may have been given permission to use for work such as; Notebooks, I-pods, I-pads, tablets and smart mobile phones.
- Personal data is any information that covers records relating to pupils and members of school staff.
- Personal data is any information held in 'structured' paper filing systems or other accessible paper records as well as computerised records.
- Once personal data becomes out of date, or no longer relevant to the purpose for which it was originally collected, it must be destroyed.
- Steps should be taken to ensure that the general public, unescorted visitors and unauthorised persons are restricted from areas where personal data is used.
- Any member of the school staff who deals with personal data as part of their job must make themselves aware of the requirements of the Act, and be familiar with how to conform to these in their daily work.
- The Data Protection Act gives any person whose personal data is held by the school, regardless of whether they are an adult or not, the right to access that data. Requests to see or receive copies of records should be made in writing to the Headteacher.
- Publication of personal information or images of individuals on any website schools develop should only be done if written consent of the individuals concerned has been given.
- E-mail should never be treated as a secure method of communication when dealing with personal data. Do not include personal data or confidential information in the text of e-mails (or attached as a data file) unless appropriate encryption is applied.
- The school will not divulge the names, addresses or other confidential information about any students or staff. Staff should be mindful that this information should not be displayed openly.
- Staff records will be held securely in the Head teacher's office.
- All confidential information relating to staff or students will be destroyed by shredding.
- Any incident involving the loss, suspected loss, or exposure of data

in electronic format either in school or externally, must be reported to the Head teacher. This means any loss of ICT equipment that stores work related files (such as laptops or memory stick).

- Losses of ICT equipment and media must be reported using the Data breach form, even if you believe that no data loss is involved.
- If the breach is considered to be negligent, Personnel will be informed.
- Personal devices must not be connected to the data network nor for the storage of school data, be that personally identifiable data or not, as they represent an unknown level of risk.
- All mobile devices require operating system and other application software updates and vulnerability patches to be applied. It is your responsibility to ensure this is done.
- If you have been given a school laptop nobody else, either at work or at home, has permission to use your allocated laptop. You will have the laptop taken from you if you don't abide by this rule.
- Remember, if you don't apply the school policies, as well as a little common sense, you may be negligent and therefore subject to legal action.
- Responsibility for ensuring that the school complies with the Data Protection Act lies with the Head teacher.