Grand Avenue Primary and Nursery School
ICT
Data management

Contents

Introduction
These three policy statements have been created to protect the interests of the school, its staff, pupils and Governors. These conditions may be changed at the discretion of the Headteacher at any time.

All staff and Governors wishing to use school ICT resources and systems need to sign a copy of the declaration contained in this document, it then being returned to school and kept on file. Once approved by the Headteacher access rights will be established. A record will be maintained of all users with system access. Users will be removed from this record when access is no longer required, in accordance with the Data protection act.

Users will be advised of any changes made to these policies.

POLICY STATEMENT 1 – Acceptable Use
The ICT facilities are owned by the school (this includes laptops allocated to individual staff) and their use is an entitlement for all authorised users subject to the conditions set out below ;

- All ICT based activity must be appropriate to a school environment
- Access to ICT resources must be made via the user's authorised account and password.
- Users will not disclose their account name and password to any other person
- Users will always log in using their own usernames and passwords
- It is forbidden to partake in any activity that threatens the integrity of the school's facilities including the use of the internet to access inappropriate materials
- The school reserves the right to monitor the use of ICT resources, emails sent or received, files held and internet sites visited at any time including examining and deleting any files held.
- Users must prepare the use of video clips and images to ensure they are appropriate before sharing with children
- Staff must always log off any computer after use

By logging on to the School's ICT resources all users agree to abide by the condition above and agree not to use them to;

- Access chat room services or download files from internet without express permission
- Publish information which could identify the user or any other person directly on any web page
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Upload, download or otherwise transmit commercial software or any copyrighted materials
- Introduce any form of computer virus into the network
- Transmit unsolicited commercial or advertising material
- Use the service to set up or run a personal business

- Post anonymous messages or send chain letters
- Broadcast unsolicited personal views on social, political or religious matters
- Represent personal opinions as those of my school or local authority
- Send pupil or staff data through unauthorised lockdowns

All users also agree to;

Seek permission from the Headteacher or ICT co-ordinator before downloading any software
Report any inadvertent access to inappropriate websites

POLICY STATEMENT 2 - TRANSFER OF SENSITIVE DATA

We aim to produce guidelines for staff to minimise a breach of data during which sensitive data may be lost, become vulnerable, altered or stolen. Sensitive data is defined as any personal or confidential information which can be linked to a specific person.

With regards to Sensitive Data staff are expected to ;

- Never create or store data which contains any client-specific information on personal devices regardless of where they intend to use the data
- Only use password protected school supplied laptops or memory sticks should they need to transport sensitive data
- Only use laptops and memory sticks as a means of transporting data on a temporary basis
- Transport data to school storage facility and delete data from laptop or memory stick as soon as it is no longer needed
- Only take sensitive physical data eg pupil file, home when absolutely necessary and with the express permission of the Headteacher.
- Never leave sensitive data/files unattended
- Maintain the confidential nature of the data wherever that data may be eg car/home. (no labels visible)
- Never read or make notes on sensitive files during a journey on public transport
- Never post images relating to school on internet or social networking sites

With regards to email staff are expected to be aware that

- The content security and safe receipt of information sent by email is always the responsibility of the sender
- Emails can be the subject of interception
- Good practice includes the use of initials rather than names, dates of birth, addresses etc..

- Normal non-secure email may be used for day to day communication with colleagues, third parties and other agencies where the nature of the information is not confidential
- Any electronic communication between staff at school and the LA which contains sensitive data should be made using a secure system called USO-FX
- Anonymised information may be sent through normal email only when extra care has been taken to verify the recipient. (e.g telephone call)
- Pupil specific reports and documents should not be sent as an attachment to an email to anyone outside the LA
- Emails should always be of a professional nature with due regard to the recipient
- No emails containing sensitive data and/or in connection with school matters should only be created and sent by staff. Sensitive data to be sent only through Atomwide

Data Breaches
On the discovery of a potential breach of data the matter should be referred immediately to the Headteacher. The Headteacher will then initiate an enquiry to ascertain the nature and scope of the breach. If it is believed that sensitive data may have been compromised then the Headteacher will notify the Information Commissioners Office and seek advice regarding subsequent action.

POLICY STATEMENT 3 – E-Safety

E-safety for pupils
All adults within the school are responsible for ensuring pupils are safe when using the internet. The ICT skills ladder contains information regarding when and how e-safety is to be discussed and taught. Teaching staff are required to follow this scheme of work.
In addition to the scheme, teachers will discuss and explain the ICT code of conduct appropriate to the age of the pupils being taught. Pupils from year 1 upwards are asked to sign a copy of the Code of conduct at the beginning of each academic year. Copies of the code are displayed in the ICT suite.

E-safety for adults
In addition to the Acceptable Use and Transfer of Data policies staff are required to use the ICT facilities sensibly, lawfully and professionally. Training in e-safety will be provided at regular intervals for all staff.

DATA MANAGEMENT POLICY

TO BE KEPT IN STAFF FILE

With regards to ICT Acceptable Use,Transfer of data and E-safety policy statements

I have read the policy statements noted above and agree to abide by the conditions.
I understand that misuse of schools ICT equipment or systems is a serious offence and could lead to disciplinary procedures

User's Name _____

User's signature_____

Headteacher signature_____

Date _____