Jump Primary School

Policies and Procedures

Information Security Policy And Acceptable Use of ICT Agreement for Staff and Governors

Jump Primary School

Information Security Policy and Acceptable Use of ICT Agreement for Staff and Governors

1. Introduction

This document:

- Sets out the general purpose of the policy.
- Identifies the individuals to whom this policy applies.
- Describes the roles and responsibilities and groups of individuals.

Barnsley MBC must operate within the law at all times. This policy and protocols must therefore be consistent with and enable actions in accordance with current legislation.

2. Scope

This policy / agreement applies to all users accessing any ICT systems (such as computers, hand held devices, or any information storing or processing devices) and information owned and/or operated by Jump Primary School. Its application extends to the use of all such equipment wherever situated.

This policy applies to everyone who reads or processes school information and applies wherever and whenever school information is processed. It applies equally to all users including:

- Teachers, Governors, Teaching Assistants, other support staff, office and premises / cleaning staff
- Contractors, consultants, casual and temporary employees and volunteers
- Partners and suppliers

Please note that throughout this document, the words “staff”, “employee” and “user” are used to cover all the groups of people listed above.

The information security policy applies to all forms of information, including, but not restricted to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned, administered or controlled by the school, including information which is:

- Spoken
- Written on paper or printed out from a computer system. This may include working both on site or remotely (e.g. at home)

- Stored on the school server, school provided Office 365 platform and the cloud
- Stored in manual filing systems
- Transmitted by electronic mail, fax, over the internet and via WiFi technology
- Stored and processed via computers, networks or mobile computing devices, including but not restricted to PCs, mobile phones, laptops, tablets and iPads
- Stored on any type or removable computer media including, but not restricted to, CDs, DVDs, USB memory sticks, external hard disks, and memory stores in devices such as digital cameras and MP3 and MP4 players.

3. Purpose

The purpose of this information security policy is:

- To protect the school's information and subsequently to protect the school's reputation
- To enable secure information sharing to deliver services
- To protect the school from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect school's employees
- NOT to constrain reasonable use of information in support of normal business activities of the school

This policy shall be seen as additional to all other school policies relating to information disclosure and personal conduct.

4. Personal and Sensitive Information

- This is defined in the supporting guidance (appendix A).

5. Managing Information Systems

5.1 Roles and Responsibilities

<u>School Governors</u>

School Governors must :-

- ensure that appropriate arrangements are in place as part of their internal control environment to ensure compliance with this Policy
- ensure that all current and new Users are aware of and undertake their roles and responsibilities and that they acknowledge this in writing.
- ensure that arrangements are made to define information systems and plans appropriate to their service as part of business continuity planning.
- undertake an annual risk assessment of the confidentiality, integrity and availability of information
- make arrangements to assure that all suppliers, contractors, partners or other organisations with access to information have the minimum requirements in place as set out in the Protocol for Data Handling for Suppliers in line with the new GDPR Regulations 25th May 2018.
- maintain an up to date inventory of all mobile devices which should be submitted annually to the Executive Director for Education in relation to schools. PC's, laptops and tablet PC's must feature on the ICT equipment register with Code Green.

Information Services

Provides advice and guidance for

- GDPR 25th May 2018
- Freedom of Information Act
- Computer Misuse Act
- Local Government (Records) Act
- Other legislation that impacts on information management e.g. Human Rights Acts, Children's Act.

Information Services is also responsible for the following matters in order to maintain information security arrangements:-

- Ensuring that information security risks are assessed and appropriate management of the risks are incorporated into new system developments
- Ensuring that advice is provided on the risks associated with the exchange of information with other organisations

Head teachers

The Supervisors are responsible for :-

- ensuring appropriate arrangements are in place to comply with this Policy and actively promoting compliance by all Users
- making sure all Users undertake appropriate training
- providing authorisation to the Code Green Service Desk of access permissions to enable all Users
- to be connected to the network,

- to be allocated an e mail address and
- to have access to appropriate information systems relevant to the role of the user.

- providing notification to the Code Green Service Desk of all changes such as leavers and movers
- reporting any identified information loss as a Data Breach which includes loss of computer equipment and mobile data devices, seeking advice from Information Services with regard to the risk associated with any proposed transfer of information to other organisations. Risk Assessments are in place to support the transfer of data in any form.
- reporting to Internal Audit a suspicion on the part of the Users which has the potential for:

- legal implications for the Council;
- to impact on services;
- by passing information security arrangements
- inappropriate usage of e-mail, Internet or other computer facilities provided by the Schools Broadband through Code Green
- the committing of fraud or corruption
- concealing any of the above

All Are Responsible For:

5.2 Information System Security

- Information shall be used legally at all times, complying with UK and European law. All users, including employees and agents of the school might be held personally responsible for any breach of the law.
- All personal information processed electronically or held in a structured manual filing system shall be processed in accordance with the General Data Protection Regulations 25th May 2018. Utmost care shall be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the school without proper authorisation.
- Personal, confidential or sensitive information shall be protected appropriately at all times and in particular when removed from school premises either physically on paper or electronic storage devices, when transmitted electronically outside the school or within areas of the school in which the public may be present.
- Information, including text, still and moving pictures, photographs, maps, diagrams, music and sound recording shall not be saved, processed or used in breach of copyright.
- The school shall only use licensed software on its computers, servers and other computing devices.
- Computers and mobile devices may not be connected to the school network,

both physically or wirelessly, without specific permission from the Headteacher. Nor shall any personally owned or non-school equipment be connected to the school computer network or to any school owned equipment, whether on the school's network or not, without written permission from the Headteacher.

- Unapproved system utilities and executable files will not be allowed to be installed or attached to emails.
- No software will be installed on or removed from Jump Primary School equipment without permission from the ICT Technician.
- Users shall not interfere with the configuration of any computing device without approval.
- School equipment, facilities and information shall be used only for school's business purposes. School equipment, facilities and information must never be used for personal gain or profit nor for electronic harassment of any kind or any action which may be to the detriment of Jump Primary School.
- School equipment, facilities and information shall be not used for private or personal interests or business.
- Files will not be removed from a shared area without specific permission, unless the retention period for the document has expired
- Staff must not log onto the school's network using someone else's user credentials (id), name and password.
- Personal data must not be stored on school servers without specific permission from the Head Teacher.
- Staff must Log Off if they are leaving the computer / room at all times, so that other staff can log in and access the network if they need to. If a number of staff are logged into a single machine it will slow down significantly.
- Teachers PC/Laptops will time out after 20 minutes and require password login.
- Office staff PC will time out after 3 minutes and will require password login.
- Unacceptable use of the school network may include, but not be restricted to:
- Wasting of resources (e.g. people, capacity, and computer).
- Alteration or destruction of the integrity of computer-based information.
- Compromising the privacy of users or confidentiality of data.

5.2 Email

- Emails sent to external organisations that are work related must be sent from a school email address.
- Staff must not let anyone else use their account nor share their password,

in school or at home.

- Personal, confidential and sensitive information sent to recipients external to the school email must be encrypted using Office 365 encryption.
- Staff must use their Jump Primary School email (Office 365) account for all emails relating to school matters.
- Staff personal e-mail addresses should not be accessible to pupils or parents.
- When teachers are responding to emails from parents/carers, responses should be courteous and brief, with the purpose of setting up a meeting. Sensitive issues should not be communicated via email.
- Any e-mails sent between staff and parents/carers should be sent through their school account and the Head Teacher should be copied in.
- If staff wish to access their school email on their own personal mobile device, a consent must be sought from the Headteacher. The personal device being used will be forced to have a device unlock code and the device will be encrypted.

5.3 Passwords

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. Passwords must always be kept private and not shared with anyone under any circumstances, including with supply staff and volunteers.
- If a password is compromised the school should be notified immediately and the password changed.
- Staff are required to change their network password - the system is set to automatically prompt the user to change their password on a 63 day programme.
- Users shall not attempt to access information to which they do not have authority.
- Passwords when reset cannot be reset again within a 15 day period.
- Accounts with a 90 day period of inactivity will expire and an engineer reset will be required.
- Passwords for websites should be entered on access every time and not remembered by the pc.
- Sims passwords are allocated to staff giving access to the areas needed dependent on the role in school. These should not be shared but can be

reset by the staff members who have system administrator rights (Business Manager/ Headteacher)

- Software programmes available in school appear on an inventory in line with data protection showing who has access to what, whether they have their own password or whether it is a school generic password. Individual passwords should not be shared. Any additional software should be incorporated to this spreadsheet and treated in the same way.

5.4 Use of the Internet and e-Safety

- Refer to the school's E-Safety policy for information on the use of the Internet and e-safety.
- Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to pupils or former pupils (see also Social Networking Policy).
- Staff members must not have contact through any personal social medium with any pupil, whether from this or any other school, unless the pupil is a family member or it is through school approved sites as part of official collaborative work (see also Social Networking Policy).
- While staff will often take photographs of children as evidence of work or to record or celebrate an event it is crucial they follow the guidelines set out by the school.

5.5 Cameras / iPads and Images of children:

- Before any school trips being filmed/photographed by outside agencies, staff must discretely identify children who do not have consent for this.
- Before any school trips being filmed/photographed by the school for use on the school website, staff must discretely identify children who do not have consent for this.
- Images of pupils on the school website must not have any names attached.
- Unless parent/carer permission is sought, images may only be used in school displays or records.
- Only cameras / iPads owned by the school may be used at school and on school trips. Parents on school trips must use school owned cameras.
- School cameras / iPads must only be used by the group of adults they have been assigned to (leads, batteries etc. must not be swapped or borrowed).
- Files on school cameras / iPads must not be downloaded onto devices not owned by the school.

- Cameras / iPads must be locked away, at school, at the end of each day, unless being used on a residential trip.
- Images may only be stored on school based devices and not on devices kept at home.
- The use of images in media publications must be approved by parents.
- Any use of webcams should be strictly monitored and only be used in planned and approved curriculum enhancement opportunities.
- Images of pupils in swimming costumes should not be used.
- The use of all images of pupils must be closely monitored by the Head Teacher and ICT co- ordinator.

5.6 Use of mobile phones:

- School owned mobiles are exclusively for work use (no personal use at all).
- Staff use of mobile phones for personal reasons is strictly restricted to non-teaching times.
- Personal calls should be made discreetly in an area which will not disturb any other members of staff or pupils.
- Mobiles should be stored away safely during teaching times
- In exceptional family circumstances, staff may need to have their mobile with them at all times in case they need to be contacted with regards to a family member. Mobiles should still be on silent and no staff member should make any calls or send texts in class. If there is a need to respond urgently, the staff member should ask another adult to take over and leave the room while they do so.
- Staff not based in class should also keep personal mobile phones on silent during their working day, so as not to disturb their colleagues' working environment and only make calls or send texts during breaks, ensuring minimal disruption to their ability to carry out their role in school.
- Personal mobile phones should always be kept on silent during any work meetings.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children or their families within or outside of the school.
- **Personal mobile phones must not be used to take or store images of children – only school cameras / iPads can be used for this.**

5.7 Use of WiFi, iPads and Tablets, Mobile Devices

- Mobile devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Teaching staff may take iPads/tablets home to be used exclusively for work purposes.
- iPads are passcode protected. No attempt must be made to disable the passcode.
- The iPads may not be used to store images of children and any images on iPads must be immediately uploaded to the Shared Drive (Non-Pupil) on the school network. These images must not be downloaded onto any other devices.
- Images may only be stored on school based devices and not on devices kept at home.

5.8 Working From Home

Staff must:

- Use only an encrypted device to transport personal and sensitive information out of school.

  Any USB stick used for personal or sensitive school information must be a school provided encrypted stick.
- Ensure that any school laptop taken home is encrypted, unless only remote access is used and no school information is stored on the hard drive.
- Always store paper and electronic information securely when away from school.
- Ensure that family members and other persons not employed by Jump Primary School do not have access to any school data.
- Not store personal or sensitive information or school owned mobile devices in the car.
- Not allow others to use school laptops or USB sticks under any circumstances.

5.9 Paper Information and Storage

Staff must:

- Ensure that all paper containing personal or sensitive information is stored securely at all times, especially in the office, and classrooms after school hours and when working from home.
- Ensure that no personal or sensitive information is displayed on classroom walls or in areas where it can be seen by the public.

5.10 Use of PCs in Classrooms

Staff must:

- Lock the screen of a PC (using Windows+L or Ctrl+Alt+Del) when leaving the PC unattended, at all times.
- Not allow anyone else to use a PC that they are logged in on.
- Not leave children unattended in the classroom using their PC.

5.11 Use of USB Sticks, Removable Memory Devices and Laptops

- Only school owned, encrypted memory sticks may be used at school and only these devices can be used to store personal and sensitive information. These must not be backed up at home. They should be backed up on individual drives on the shared network.
- If any school owned devices (memory sticks, cameras tablets etc.) are lost or stolen it must be reported immediately to a member of the SLT.
- Adequate protection must be given to any device holding sensitive or personal data to prevent unauthorised access.
- School laptops will be encrypted if they contain personal or sensitive information.
- Tablets and laptops **which have been encrypted** may be taken home and **used for work purposes only**. If they are lost or stolen it must be reported to a member of SLT immediately. These devices must be in school for every school day as they are also used to support children's learning in class.

6. Breaches of Information Security

Actions or neglect leading to a breach of this policy will be investigated, which could result in disciplinary action; this could include dismissal without notice even for a first offence if sufficiently serious.

Any actual or suspected breaches of any security policy within, or affecting, Jump Primary School's systems will be thoroughly investigated by the Headteacher and the Data Protection Officer. If staff are involved, disciplinary action (following current agreed disciplinary procedures) may be taken. Any action taken internally does not preclude prosecution through a court of law.

Breaches of this policy by a user who is not a direct employee of the school may result in action being taken against the user and/or their employer.

In certain circumstances the matter will be referred to the police to consider whether criminal proceedings should be instigated.

Breaches of the General Data Protection Regulations 2018 could result in a large fine being issued to or criminal proceedings taken against the individual or the school.

7.1 Use of the ICT technician's or co-ordinator's time:

Staff may not use the working time of the technician's or co-ordinator to support them with any ICT advice or support which is not directly linked to school business. They will not be available to mend or maintain any devices not used by the school. If damage or maintenance to any school equipment is required due to non-school business the person responsible for that damage will liable for any costs incurred in delivering the required repairs or maintenance.

The time of the ICT technician will be managed and directed by the Headteacher and the Business Manager. Requests for ICT support can be made through the ICT Logbook, on the shared network . The ICT co-ordinator and the technician will prioritise requests based on school priorities.

8.1 Responsibilities for saving energy and resources:

All staff must take responsibility for saving energy and resources with regards to ICT. This includes:

- Turning off projectors after school.
- Turning off all devices at the end of the day.
- Monitoring pupil activity appropriately to ensure resources are not wasted.

9. Compliance

This policy has been issued with the authority of the Head Teacher and governors and compliance with its principles is mandatory for all employees of Jump Primary School and authorised third party users accessing any computer system owned or operated by the school.

10. Definition

All references in this document to the 'school' shall be deemed to refer to Jump Primary School.

11. Interpretation

In the event of an issue arising from an interpretation of this policy, it should be resolved by reference to the Head Teacher and ICT co-ordinator.

12. Reference Documents:

- E-safety Policy

- Social Networking Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy

Appendix A Supporting guidance

Why should your data be secure?

One of the 6 principles of GDPR specifies that the data must be kept securely.

What data should be secure?

For ease of understanding your data we have given some examples of data and the security measures required to protect them. The examples given are just that, they are not exhaustive lists and the security required depends on the volume of data as well as the sensitivity. For example, the medical records of the whole school require different security considerations to the medical records of a single pupil.

The following categories are for demonstration purposes only.

Red data (those that contain very personal details)

- EHCP's and IEPs
- Education Psychologist reports
- Education Welfare Officer reports
- Medical records
- Personnel records
- SEN registers
- Accessing your Management Information System or admin servers
- Financial information concerning staff pay
- Staff personnel records

Amber data (data that contains personal data that if lost could identify individuals)

- Names and Addresses
- Parental and staff contacts
- Pupil reports
- Exam results

Green data (data that does not identify individuals)

- Lesson plans
- Class lists (if only showing initials or forenames)

- Curriculum plans
- General marking

If you don't mind it being available on a website or in the local paper then it is green data

What is Personal and Sensitive Information?

Personal information is:

- Defined as any combination of data items that identifies an individual and provides specific information about them, their achievements and their families
- That could include: names, contact details, gender, dates of birth, unique pupil number etc.
- It could also include: academic achievements, skills and abilities, progress, behaviour and attendance

Sensitive data is specifically defined as information relating to:

- a person's racial or ethnic origin
- political opinions
- religion or beliefs
- membership of a trade union
- physical or mental health
- sexual life
- alleged offence or any proceedings for any offence

By its nature this information needs to be treated with greater care than other personal data.

Further Guidance on Managing Information Systems

- The Headteacher is the Senior Information Risk Owner (SIRO).
- The schools server will be backed up each night and stored securely.
- Security strategies will be discussed with Traded Services - Code Green regularly.
- Anti-virus protection will be updated regularly. Staff with school laptops will have anti-virus protection installed by the ICT technician which will update at home if it is connected to the internet. If not connected to the internet, then staff will need to log on to their laptop at school to update on a regular basis.
- The security of individual staff and pupil accounts will be reviewed regularly. Both staff and pupils must be informed of the importance of not sharing passwords.
- The administrator account password will be changed if it becomes known.
- Staff have secure areas on the network to store personal or sensitive files.

- Details of school owned hardware will be recorded in a hardware inventory.
- The ICT coordinator and ICT technician will review system capacity regularly.
- Jump supply accounts must be used for short term visitors for temporary access to appropriate systems.
- Employees must not install or use any encryption software other than that provided by the school
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Further guidance on email and passwords:

- Email addresses should be published carefully, to avoid email harvesting for spam purposes.
- Strong passwords must be used on the school network i.e. it must contain lower case and upper case letters, numbers and special characters
- Staff using critical systems, such as CPOMS, must use two factor authentication.
- The Office will give details of the restricted Supply log-in and password to any supply teachers.

Printing

Staff must:

- When printing personal or confidential material, ensure that a secure printing method is used.
- Not leave personal or sensitive information on the printer, it must be collected from the printer as soon as it is printed.
- Not send children to collect documents from the printer if it includes sensitive data.

Retention of Data and Data Disposal

- Information must be stored in accordance with the General Data Protection Regulations 2018 and must not be stored for any longer than stated in the retention schedule.

Use of Website and Storage of Data in the 'Cloud'

- The school website shall only be used to promote the school, the education of our pupils and communication with parents/carers and the wider community. All content is strictly controlled and monitored by the Head Teacher and ICT co-ordinator.
- The school website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- No personal or sensitive information may be stored in the cloud.

Review of the Information Security Policy

This document shall be reviewed on a regular basis and at least annually. This policy and any associated policies shall be updated according to:

- Internally generated changes such as changes in service strategy, organisations, locations and technology.
- Externally generated changes such as changes in legislation, security threats, security incidents, recommended best practice and audit reports.
- All changes shall be approved by the Head Teacher and School Governors and be made available to everyone to whom it applies.